# Belgium

Boulet, Gertjan; de Hert, Paul

*Published in:*
Access to telecommunication data in criminal justice

*Publication date:*
2016

*Document Version*
Peer reviewed version

# Belgium*

National Rapporteurs:
*Gertjan Boulet*
*Paul De Hert*

* This report reflects legislation and case law as of September 2016.

# Contents

# I. Security Architecture and the Interception of Telecommunication

## A. Law Enforcement Institutions and Security Services with Powers of Telecommunication Interception

### 1. National security architecture

The Belgian national security architecture includes (preventive) police law, (preventive and reactive) criminal law, and intelligence (state security) law. All of these legal regimes provide coercive powers for the interception of electronic communications.

The prerequisites under general police law for the interception of electronic communications differ from the other legal regimes, which contain stricter rules and authorization, more particularly: in criminal law, prior authorization by the public prosecutor (during the preliminary investigation/inquiry phase, or during the investigation/instruction phase) or by the investigating judge (during the investigation/instruction phase); in intelligence law, prior authorization (for exceptional intelligence collection methods) or *a posteriori* authorization (for specific intelligence collection methods) by the administrative commission responsible for monitoring the specific and exceptional intelligence collection methods used by the intelligence and security services (SIM commission).

The prerequisites for the interception of the content of communication in transmission under criminal law and intelligence law are largely similar.[1] However, the interception powers under intelligence law provide special protection for journalists, unlike the interception powers under criminal law.

---

[1] Article 90*ter* of the Code of Criminal Procedure, and Article 18/2 §2, 7° of the Act of 30 November 1998 on the Intelligence and Security Services.

## 2. Powers for the interception of telecommunication[2]

### *a) Law of criminal procedure*

#### aa) Normal investigation methods

The legal provisions for intercepting electronic communications under (reactive) criminal law are provided in the Code of Criminal Procedure (hereinafter: CCP): data seizure (Article 39*bis* CCP), the collection of identification data of electronic communications (Article 46*bis* CCP), tracing of traffic data, and localization of electronic communications (Article 88*bis* CCP), the network search (Article 88*ter* CCP), and wiretapping/monitoring, including direct monitoring/eavesdropping[3] (Article 90*ter* §1 CCP).

#### bb) Special investigation methods and any other methods of investigation

The Act of 6 January 2003 concerning special investigation methods and any other methods of investigation[4] introduced three *special investigation methods* and five *other investigation methods* into the CCP.

The two *special investigation methods* relevant for the interception of electronic communications are observation (Article 47*sexies* CCP) and infiltration (Article 47*octies* CCP).

The two *other investigation methods* relevant for the interception of electronic communications are looking-in operations (Article 46*quinquies* and 89*ter* CCP), and the power to enter a house or a private place to enable eavesdropping with technical means (Article 90*ter* §1, 2° CCP). Hereinafter, we use the term monitoring measure to refer to both the general wiretapping measure under Article 90*ter* §1, 1° CCP and the measure to enter a house or a private place to enable eavesdropping with technical means under Article 90*ter* §1, 2° CCP.

---

[2] The answers to the questions under this section are partially based on Gertjan Boulet's contribution to an EU-funded project on surveillance: Gertjan Boulet, "Regulating Surveillance: The Belgian case," Deliverable 2.3 (The Legal Perspective) for the EU-funded project Increasing Resilience in Surveillance Studies (IRISS), pp. 49–52, 31 January 2013, available at http://irissproject.eu/wp-content/uploads/2013/04/Legal-perspectives-of-surveillance-and-democracy-report-D2.3-IRISS.pdf.

[3] The monitoring measure in Article 90*ter* §1, 1° CCP also covers direct eavesdropping from outside a home or private place. Article 90*ter* §1, 2° CCP, however, describes the power to enter a house or a private place to enable eavesdropping by technical means. See Chris Van den Wyngaert, *Strafrecht, Strafprocesrecht & Internationaal Strafrecht in hoofdlijnen* (An Outline of Criminal Law, Criminal Procedural Law & International Criminal Law), Antwerp-Apeldoorn, Maklu, 2006, p. 982, footnote 4012.

[4] Act of 6 January 2003 concerning special investigation methods and any other methods of investigation, *Belgian Official Journal*, 12 May 2003, entry into force on 22 May 2003.

### cc) Cooperation with individuals and the private sector

For the execution of the above-mentioned investigation operations, Belgian law enforcement agencies can cooperate with individuals and the private sector (Article 39*bis*, Article 46*bis*, Article 88*bis*, Article 88*quater*, Article 90*quater* §§2, 4 CCP). Belgian law enforcement agencies can also cooperate with so-called closed user groups,[5] on the basis of Articles 122, 125, and 127 of the Electronic Communications Act,[6] and with service providers acting as a mere conduit, catching, and hosting on the basis of Articles XII.17 to XII.20 of the Code of Economic Law.[7] Furthermore, in specific cases, judicial authorities can order a temporary surveillance period for Internet service providers acting as a mere conduit, catching, and hosting (Article XII.20 of the Code of Economic Law).

### dd) Data retention

The general data retention (preservation) provision is Article 126 of the Electronic Communications Act of 13 June 2005.[8] However, on 11 June 2015, the Belgian Constitutional Court invalidated Article 126 of the Electronic Communications Act. A new Belgian data retention law of 29 May 2016 entered into force on 28 July 2016.[9]

A Royal Decree of 19 September 2013 lists the types of data subject to data retention.[10] Article 9 §7 of the Electronic Communications Act provides that a specific Royal Decree shall address the matter of data retention for closed user groups.

---

[5] Article 9 §5-6 of the Electronic Communications Act provides that the duty to notify the Belgian Institute for Postal Services and Telecommunications does not apply to providers and resellers of electronic communications networks or services not exceeding the public domain (§5), or to providers and resellers of electronic communications networks or services either exclusively targeted at legal entities in which the provider or seller has a controlling interest, or provided to a natural or legal persons as mere support and accessory (§6).

[6] Article 9 §7 of the Electronic Communications Act of 13 June 2005 provides that a specific Royal Decree shall address the matter of the cooperation between law enforcement agencies and closed user groups: Act of 13 June 2005 on electronic communications, *Belgian Official Journal*, 20 June 2005, entry into force on 30 June 2005.

[7] The Code of Economic Law of 28 February 2013, *Belgian Official Journal*, 29 March 2013, entry into force on 12 December 2013.

[8] As amended by the Belgian Communication Act of 30 July 2013 amending Articles 2, 126, and 145 of the Act of 13 June 2005 on electronic communications and Article 90d*ecies* of the Code of Criminal Procedure, *Belgian Official Journal*, 23 August 2013, entry into force on 2 September 2013.

[9] Act of 29 May 2016 on the collection and retention of data in the electronic communications sector, *Belgian Official Journal*, 18 July 2016, entry into force on 28 July 2016.

[10] Royal Decree of 19 September 2013 regarding the execution of Article 126 of the Act of 13 June 2005 on electronic communications, *Belgian Official Journal*, 8 October 2013, entry into force on 19 September 2013.

Federal Magistrate Jan Kerkhofs and Investigating Judge Philippe Van Linthout argue that Belgian providers of electronic communication services or networks, with no notification duty, are currently released from data retention obligations, taking into account the lack of a specific Royal Decree.[11] For the same reason, the service providers that act as a mere conduit or provide caching and hosting activities under the Code of Economic Law are currently released from data retention obligations.

Finally, notaries, bailiffs, and accountants are subject to specific data retention and production obligations, provided in Article 7 and under chapter III of the Law of 11 January 1993 on preventing misuse of the financial system for purposes of laundering money and terrorism financing.[12]

### *b) Preventive law*

The legal provisions for intercepting electronic communications under (preventive) police law are the general provision on crime detection and evidence gathering by the police (Article 8 CCP), and a specific provision on access by the police to publicly accessible places (Article 26 of the Act on the Police Function).[13]

The legal provision for intercepting electronic communications under (preventive) criminal law is the provision on proactive investigation (Article 28*bis* §2 CCP), which reads as follows:[14]

> §2. The preliminary investigation extends to proactive investigation. This is understood, in order to prosecute perpetrators of criminal offences, the detection, collection, recording and processing of data and intelligence on the basis of a reasonable presumption of punishable acts yet to be committed or already committed but not yet discovered, and that are or would be committed in the framework of a criminal organization as defined by law, or constitute or would constitute crimes or misdemeanours referred to in Article 90ter, §§2, 3 and 4. The use of proactive investigation requires prior written approval by the public prosecutor, the labour prosecutor (or the federal prosecutor) given under their respective jurisdiction, without prejudice to compliance with the specific legal provisions that regulate special investigative methods and other methods.

Delbrouck (attorney-at-law) underlines that the coercive powers of wiretapping, observation, and entering private places within the framework of a looking-in operation cannot be used by the public prosecutor during the preliminary investigation

---

[11] Jan Kerkhofs and Philippe Van Linthout, *Cybercrime*, Brussels, Politeia, 2013, p. 396.

[12] Act of 11 January 1993 on preventing use of the financial system for purposes of laundering money and terrorism financing, *Belgian Official Journal*, 9 February 1993, entry into force on 1 December 1993, available at http://www.imolin.org/doc/amlid/Belgium_law_11_January_1993.pdf

[13] Act of 5 August 1992 on the Police Function, *Belgian Official Journal*, 22 December 1992, entry into force on 1 March 1993.

[14] Author's own translation of the Belgian law related to the interception of electronic communications. All subsequent translations of statutory texts are the author's own.

phase, hence also not during proactive investigation, on the basis of Article 28*septies* CCP, which explains the so-called legal notion of mini-instruction:[15]

> The public prosecutor can request the investigating judge, without the initiation of a judicial investigation, to perform any investigative measure for which only the investigating judge is competent, with the exception of an arrest warrant provided in Article 16 of the Law of 20 July 1990 on remand custody, the fully anonymous testimony referred to in Article 86bis, the monitoring measure referred to in Article 90ter [interception], the investigative measures referred to in Article 56bis, second paragraph [observation] and 89ter [looking-in operations] and the house search. After the execution of the investigative measure carried out by the investigating judge, he shall decide whether to return the file to the public prosecutor responsible for the continuation of the investigation or to continue the whole investigation himself, in which case one shall further act in accordance with the provisions of Chapter VI of this book. This decision cannot be appealed.

Furthermore, Kennes (attorney-at-law) notes that, whereas the proactive investigation can be activated following a "reasonable presumption of punishable acts," the monitoring measure (Article 90*ter* CCP) is reserved for cases in which there are "serious indications that the offense is a criminal offense."[16]

Van den Wyngaert, however, notes that the distinction between proactive and reactive investigation is not always an easy one to draw and that the European Court of Human Rights (ECtHR) in the case *Lüdi v. Switzerland*[17] held that a proactive wiretapping measure, if based on law, is not incompatible with the European Convention on Human Rights (ECHR).[18]

### *c) Law of intelligence agencies*

The legal provisions for intercepting electronic communications under intelligence law are provided in the Act of 30 November 1998 on the Intelligence and Security Services.[19] Ordinary collection methods include: intelligence collection with private actors (Article 16), observation and search without technical means of public places and private places accessible to the public (Article 16/1).

---

[15] Luk Delbrouck, "De proactieve recherche: een nieuw middel in de strijd tegen de georganiseerde criminaliteit?" (The proactive investigation: a new method in the fight against organized crime), *Jura Falconis*, 1999-2000, no. 1, pp. 121–158, available at https://www.law.kuleuven.be/jura/art/36n1/delbrouck.htm#N_136_

[16] Laurent Kennes, *Manuel de la preuve en matière pénale* (Manual on evidence in criminal matters), Mechelen, Kluwer, 2009, p. 209.

[17] ECtHR, *Lüdi v. Switzerland*, 15 June 1992, Grand Chamber, no. 12433/86, via http://hudoc.echr.coe.int/

[18] Chris Van den Wyngaert, *Strafrecht, Strafprocesrecht & Internationaal Strafrecht in hoofdlijnen* (An Outline of Criminal Law, Criminal Procedural Law & International Criminal Law), Antwerp-Apeldoorn, Maklu, 2006, pp. 683, 843, 986, footnote 4399.

[19] Act of 30 November 1998 Law on the Intelligence and Security Services, *Belgian Official Journal*, 18 December 1998, entry into force on 1 February 1999.

Specific collection methods include: observation or searches with technical means of public places and private places accessible to the public, observation with or without technical means of private places not accessible to the public (Article 18/2 §1, 1° and 2°; specified in Articles 18/4, 18/5), collection of identification data of electronic communications (Article 18/2 §1, 4°; specified in Article 18/7), the tracing of traffic data, and localization of electronic communications (Article 18/2 §1, 5°; specified in Article 18/8).

Exceptional collection methods include: observation with or without technical means *in* private places not accessible to the public, or in houses (Article 18/2 §2, 1°; specified in Article 18/11), a search with or without technical means of private places not accessible to the public, or houses (Article 18/2 §2, 2°; specified in Article 18/12), the collection of banking data (Article 18/2 §2, 5°; specified in Article 18/15), intrusion into a computer system (Article 18/2 §2, 6°; specified in Article 18/16), and wiretapping (Article 18/2 §2, 7°; specified in Article 18/17).

An additional collection method concerns the power for the (military) General Intelligence and Security Service of the Armed Forces (GISS) to intercept communications transmitted from abroad (Article 44*bis*).

For the execution of the above-mentioned intelligence operations, Belgian intelligence agencies can cooperate with individuals and the private sector (Article 16, Article 18/7, Article 18/8, Article 18/16, Article 18/17 of the Act of 30 November 1998 on the Intelligence and Security Services).

### *d) Customs Investigation Service*

Belgian Customs Investigation Services have no powers to intercept electronic communications under Belgian law. Cybersquad, falling under the investigation services of the General Administration Customs and Excise (Federal Public Service Finance),[20] has powers, among others, to block websites offering illegal goods.[21] The Belgian Internet Service Center (BISC), established in 2011 under the Federal Public Service Finance's General Administration's Special Tax Inspectorate,[22] has powers to investigate Internet fraud: it detects infringements of Belgian law by

---

[20] Federal Overheidsdienst Financiën, Algemene Administratie der douane en accijnzen (in Dutch), Service Public Fédéral Finances, Administration générale des doaunes et accises (in French).

[21] A project leader at Cybersquad presented the functions of Cybersquad in a presentation (September 2012): available at https://www.b-ccentre.be/wp-content/uploads/2012/04/Cybersqu@d-28maart2012-v005.pdf

[22] Bijzondere Belastinginspectie (BBI, in Dutch), Inspection spéciale des impôts (ISI, in French).

online shops offering goods in Belgium and controls domain names with the extension .be. BISC also possesses software to map suspicious websites.[23]

### 3. Responsibility for the technical performance of interception measures

#### *a) Material competence*

The responsibility for the technical performance of interception measures under police law lies with the judicial police.

The responsibility for the technical performance of interception measures under (preventive) criminal law lies with the public prosecutor.

The responsibility for the technical performance of interception measures under (reactive) criminal law lies with the investigating judge, the public prosecutor, and judicial police officers.

The responsibility for the technical performance of interception measures under intelligence law lies with both the Director-General of the intelligence and security agencies and the administrative commission responsible for monitoring the specific and exceptional intelligence collection methods used by the intelligence and security services (SIM commission).

#### *b) Territorial competence*

The police and law enforcement agencies are structured at the federal and local levels. The intelligence agencies are structured at the federal level. There is one federal public prosecutor. The local public prosecutor's offices are situated at the same level as the Courts of First Instance: the judicial districts. The 2014 judicial reform reduced the judicial arrondissements (districts) from 27 to 12, of which the boundaries overlap with nine of the 10 provinces (West Flanders, East Flanders, Antwerp, Limburg, Hainaut, Namur, Walloon Brabant, Liège, Luxembourg) and the cities Leuven (province Flemish Brabant), Brussels (province Flemish Brabant), and Eupen for German-speaking Belgium (part of the province Liège).[24]

---

[23] Christina Bourlet, "La lutte contre la fraude de mass: développements récents" (the fight against mass fraud: recent developments), in Dominique Grisay (ed.), *De la lutte contre la fraude à l'argent du crime: État des lieux*, Brussels, Groupe De Boeck, 2013, pp. 83–98.

[24] The rationale behind the division into 27 districts, dating back to the foundation of Belgium in 1831, is that every capital city in each district be reachable by horse in one day. On the judicial reform in Belgium, see Stefaan Voet, "Belgium's new specialized judiciary," *Russian Law Journal*, 2014, vol. II, issue 4, pp. (129) 130, 138, available at http://www.russianlawjournal.org/index.php/jour/article/view/14/10

The law of 19 July 2012 on the reform of the judicial arrondissement Brussels[25] split up the public prosecutor's office covering the area Brussels-Halle-Vilvoorde.[26] The law of 19 July 2012 created, on the one hand, a public prosecutor's office covering the administrative arrondissement of Brussels-Capital and, on the other hand, a public prosecutor's office covering the administrative arrondissement Halle-Vilvoorde. In other words, a public prosecutor's office was created for the administrative district of Brussels-Capital, which covers the bilingual (French and Dutch) 19 municipalities of the Brussels-Capital Region (better known as Brussels); another public prosecutor's office was created for the administrative district Halle-Vilvoorde, which surrounds Brussels and consists of 35 Dutch-speaking municipalities that have language facilities.

The local Prosecutor General's offices are situated at the same level as the courts of appeal, more particularly at the five judicial areas (Ghent, Brussels, Antwerp, Mons, Liège).

The federal Prosecutor General's office is situated at the level of the Supreme Court.

The investigating judges are situated at the Courts of First Instance and are appointed by the King from among the judges at the Courts of First Instance.

#### *c) Cooperation with individuals and the private sector*

As mentioned above (section I.A.2.), for the execution of investigation and intelligence operations, Belgian law enforcement agencies and intelligence agencies can cooperate with individuals and the private sector.

### 4. Legitimacy of data transfers between different security agencies

There is a separation between the various institutions responsible for the interception of electronic communications under the police law, criminal law, and intelligence law. Thus, there are no joint agencies that carry out interception.

However, the results of interception measures under these different legal regimes can be exchanged between the competent authorities.

---

[25] Law of 19 July 2012 on the reform of the judicial district Brussels, *Belgian Official Journal*, 22 August 2012, entry into force (almost two years later) on 31 March 2014.

[26] The area Brussels-Halle-Vilvoorde was not only covered by the "judicial district" of Brussels, but also by the "electoral district" of Brussels.

### *a) Exchange of data between law enforcement authorities and preventive police authorities*

There are several provisions that imply data exchanges from police authorities to law enforcement authorities.

First, Article 29 CCP provides that any authority shall immediately inform the public prosecutor of a crime or misdemeanour that comes to its knowledge. This article also applies to the intelligence and security services (see I.A.4.b. below) and is echoed by Article 44/1 §3 of the Act of 5 August 1992 on the Police Function.

Second, Article 28*bis* §1 CCP provides that preliminary investigations be conducted under the direction and authority of the competent public prosecutor. This is confirmed by Article 6 of the Act of 5 August 1992 on the Police Function.

Third, Article 15, 1° of the Act of 5 August 1992 on the Police Function reads as follows:

> In the performance of their judicial police functions, the police have the task: 1° to detect the crimes, misdemeanours and contraventions, to gather evidence thereof, to notify the competent authorities thereof, to apprehend and arrest the perpetrators, to bring them at the disposal of the competent authorities, in the manner and forms provided by law;

Article 53 CCP adds that the judicial police officers shall immediately send the reports (of an offense), official records,[27] and any other acts drafted under their competence to the public prosecutor. This provision is echoed by Article 40 of the Act of 5 August 1992 on the Police Function, which provides that police officers shall send official records on complaints, reports of offenses, and intelligence and any detections to the competent judicial authorities.

Article 54 CCP adds that the judicial police officers shall also immediately send any reports of crimes and misdemeanours they are not competent to detect to the public prosecutor.

Article 5/3 of Act of 5 August 1992 on the Police Function adds that, for the performance of judicial police functions, the police shall maintain regular *service relations* with the local public prosecutors, the federal public prosecutor, and the Prosecutors General.

Third, the project "Autonomic Police Treatment" (APT)[28] allows for independent police treatment in specific cases. Article 28*bis* §1, 2° CCP provides that the

---

[27] Proces-verbaal (in Dutch), procès-verbal (in French).

[28] Previously called Autonome Politionele Afhandeling (APA, in Dutch), or le Traitement Policier Autonome (in French); currently called Ambtshalve Politioneel Onderzoek (APO), or Enquête Policière d'Office (in French). For a government-funded research project on the opportunity of APT and the evaluation of its effectiveness, see Federal Science Policy Office (BELSPO), "Stated goals van autonome afhandeling door de politie (APA): zijn ze opportuun en worden ze bereikt?" (Stated goals of the Autonomic Police Treatment: are they opportune and are they achieved?), SO/02/016, research project from 1 De-

law and special rules issued via circular by the Board of Prosecutors General[29] determine the general principles for APT. The circular of 15 June 2005 issued by the Board of Prosecutors General lays down the rules on APT and the simplified official record (see below under this section).[30]

Although Article 28*bis* §1, 3° CCP confirms that the preliminary investigations are conducted under the direction and authority of the competent public prosecutor, Ponsaers and other members of a research project on APT explain that APT "breaks with the tradition of the public prosecutor as a mere sender and receiver of instructions (a 'letter-box'); all necessary police research should be finished before the file can be sent to the public prosecutor's office."[31] The authors further refer to the wording of Article 28*ter* §2 CCP, which provides that judicial police officers and agents acting on their own initiative shall inform the public prosecutor of the conducted investigations *within the time and in the manner provided by the public prosecutor in a directive (circular)* (italics added). They see APT as a *manner* for the public prosecutor to realize investigation policy. In this manner, Article 28*ter* §4 CCP provides that the police, designated by the public prosecutor to perform judicial police functions, shall immediately inform the latter of the information and intelligence in its possession, and of every conducted investigation *in the manner provided by the public prosecutor* (italics added). The authors also refer to a judgment of the Supreme Court of 21 August 2001,[32] which confirms the possibility of APT without prior notification of the public prosecutor. The Supreme Court also held that the notification duty laid down in Article 28*ter* CCP is not substantial and not prescribed under penalty of nullity.

Fourth, the police principally do not forward simplified official records, which are used for relatively non-serious offenses,[33] to the public prosecutor. The police only send a monthly list to the public prosecutor, which contains the number of the simplified official records; a short description of the offense; the qualification,

---

cember 2000 till 28 February 2003, available via http://www.belspo.be/belspo/fedra/proj.asp?l=nl&COD=SO%2F02%2F016

[29] The Board of Prosecutors General (*College van procureurs-generaal* in Dutch; *Collège des procureurs généraux* in French) can take measures to ensure a coherent implementation and coordination of criminal policy as determined in ministerial directives and the well general and coordinated functioning of the public prosecutor's office (Article 143*bis* §2 of the Judicial Code).

[30] Board of Prosecutors General, Circular of 15 June 2005 regarding the Autonomic Police Treatment and the simplified official records, COL 8, available (in Dutch and French) at http://www.om-mp.be/omzendbrief/4016820/omzendbrief_col_8_d_d__15_06_2005.html

[31] See the English summary of the APT project: "Policing: Relative Autonomy? An empirical research into Autonomic Police Action," available at http://www.belspo.be/belspo/organisation/publ/pub_ostc/SoCoh/rSO02016_en.pdf

[32] Supreme Court, 21 August 2011, P.01.1203.F/1, available via http://jure.juridat.just.fgov.be/

[33] Vereenvoudigd proces-verbaal (in Dutch), procès-verbal simplifié (in French).

place, and time of the offense; and the identity of the implicated persons. As mentioned earlier under this section, the circular of 15 June 2005 issued by the Board of Prosecutors General lays down the rules on APT and simplified official records.[34]

*b) Passing on of data by intelligence agencies*

Regarding information transfers from the intelligence and security services to the police services, Article 20 §1 of the Act of 30 November 1998 on the Intelligence and Security Services lays down a general obligation of maximum efficient mutual cooperation between intelligence and security services, police services, and administrative and judicial authorities.

Furthermore, the Act of 18 March 2014 inserted a new Article 44/11/9 into the Act of 5 August 1992 on the Police Function, §4 of which lays down a duty for the intelligence and security services and other services to transfer data and information, which are processed within the framework of their functions and that are sufficient, relevant, and not excessive in view of police functions, to the police services.

Regarding information transfers from the intelligence and security services to the judicial authorities, there are three ways to transfer information.

First, Article 19/1 §1 of the Act of 30 November 1998 on the Intelligence and Security Services provides that, in view of the application of Article 29 CCP, these services shall immediately inform the administrative commission responsible for monitoring the specific and exceptional intelligence collection methods used by the intelligence and security services (SIM commission) if the performance of specific or exceptional collection methods reveals serious indications of the commission of a crime or misdemeanor, or, in case of reasonable suspicion, of unrevealed or future offenses. As said, Article 29 CCP provides that any authority shall immediately inform the public prosecutor of a crime or misdemeanor that comes to its knowledge (see section I.A.4.a. above). This article also applies to the intelligence and security services.

Article 19/1 §2 of the Act of 30 November 1998 on the Intelligence and Security Services provides that, if the SIM commission confirms the findings of the intelligence and security services, then the president of the SIM commission shall draft an *unclassified* official record and immediately send it to the public prosecutor or the federal prosecutor after having heard the Director-General of the intelligence and security agencies regarding the conditions of the transfer.

---

[34] Board of Prosecutors General, Circular of 15 June 2005, COL 8, available (in Dutch and French) at http://www.om-mp.be/omzendbrief/4016820/omzendbrief_col_8_d_d__15_06_2005.html

Second, Article 20 §1 of the Act of 30 November 1998 on the Intelligence and Security Services lays down a general obligation of maximum efficient mutual cooperation between intelligence and security services, police services, and administrative and judicial authorities. Article 20 §2 of the Act of 30 November 1998 on the Intelligence and Security Services provides that the intelligence and security services *can* cooperate with the judicial and administrative authorities, upon their request, and within the limits of a protocol adopted by the relevant ministers.

Article 19 provides that the intelligence and security services shall *only* transfer intelligence to the concerned ministers or judicial and administrative authorities, the police services, and all competent organizations and persons according to the purposes of their functions and in relation to threatened organizations and persons.

A service note of the Federal Prosecutor of 17 December 2012 on the written information exchanges between the intelligence and security services and the public prosecutor is based on the unpublished circular COL 9/2012 of 21 June 2012 of the Board of Prosecutors General regarding the Act of 30 November 1998 on the Intelligence and Security Services; it determines the principles regarding the use and preservation of classified information at the federal public prosecutor's office.[35]

For the data transfer from intelligence agencies to judicial authorities, there is no similar provision to Article 14 §1-2 of the Act of 30 November 1998 on the Intelligence and Security Services, which allows information transfers from judicial authorities and police service, *on their own initiative*, to intelligence and security services (see I.A.4.c. below).

Third, there is an additional information flow from the oversight body of the intelligence agencies, i.e., the Belgian Standing Intelligence Agencies Review Committee (Standing Committee I), to the judicial authorities. The Standing Committee I acts as a prejudicial advisor in case the Council Chamber[36] (Article 131*bis* CCP) or the court dealing with the substance of the case (Article 189*quater* CCP) or the Court of Assize (Article 279*bis* CCP), when confronted with an unclassified official record as referred to in Article 19/1 of the Act of 30 November 1998 on the Intelligence and Security Services, requests the advice of the Standing Committee I on the legality of the collection methods used by the intelligence services.

---

[35] Federal Prosecutor's Office, Annual report of the Public Prosecutor's Office to the Board of Prosecutors General for the period 1 January 2012 till 23 December 2012, 2012, p. 124, available (in Dutch) at http://www.om-mp.be/images/upload_dir/jaarverslag2012.pdf

[36] The Council Chamber (*Raadkamer* in Dutch; *Chambre du conseil* in French) supervises the investigation phase at the Court of First Instance. The Indictment Chamber or Court of Indictment (*Kamer van Inbeschuldigingstelling* in Dutch; *Chambre des mises en accusation* in French) supervises the investigation phase at the Court of Appeal.

*c) Passing on of data to intelligence agencies*

Regarding the transfer of information from the police services and judicial authorities to the intelligence and security services, first, Article 20 §1 of the Act of 30 November 1998 on the Intelligence and Security Services lays down a general obligation of maximum efficient mutual cooperation between intelligence and security services, police services, and administrative and judicial authorities.

Second, Article 14 §1-2 of the Act of 30 November 1998 on the Intelligence and Security Services provides that the civil servants and agents of public services (including police services) and judicial authorities, can transfer information that is useful for the functions of the intelligence and security services, on their own initiative or upon request, while considering the law, and on the basis of potentially concluded agreements or hierarchical rules. Article 14 §2 of the Act of 30 November 1998 on the Intelligence and Security Services provides that the civil servants and agents of public services (including police services) and judicial authorities can refuse to transfer information, if they deem that such a transfer would compromise an ongoing (preliminary) investigation or the collection of information according to the law of 11 January 1993 on preventing misuse of the financial system for purposes of laundering money and terrorism financing, or if it could harm someone in his or her personal physical integrity.

## B. Statistics on Telecommunication Interception

### 1. Obligation to collect statistics

There is an obligation for law enforcement authorities and courts to report statistics to the Ministry of Justice. Article 90*decies* CCP provides that the Minister of Justice will report annually to the Parliament on the application of some but not all investigation methods:

> The Minister of Justice will report annually to the Parliament on the application of Articles 90ter to 90novies.
>
> He informs the Parliament of the number of investigations which gave rise to the measures referred to in those articles, the duration of these measures, the number of persons involved and the results obtained.
>
> He also reports on the application of Articles 40bis, 46ter, 46quater, 47ter to 47decies, 56bis, 86bis, 86ter, 88sexies and 89ter.
>
> He informs the Parliament of the number of investigations which gave rise to the measures referred to in these articles, the number of affected persons, the offenses to which they relate and the results obtained.
>
> He also reports on the application of Articles 102 to 111 and 317 and notifies the Federal Parliament of the number of cases involved, persons and crimes.
>
> This report is also complemented by the report prepared pursuant to Article 126, §6, third paragraph, of the Act of 13 June 2005 on electronic communications.

This report is also complemented by the report prepared pursuant to Article 126, §5, fourth paragraph, of the Act of 13 June 2005 on electronic communications.

The annual reports of the Minister of Justice in implementation of Article 90*decies* CCP[37] provide that data collection and processing is determined via the confidential circular COL 17/2006 of the Board of Prosecutors General. The annual reports of the Minister of Justice in implementation of Article 90*decies* CCP disclose some explanations about the general procedure and the data collection. The reports provide details about the providers of information: the federal police provides data regarding the power to enter a house or a private place in order to enable eavesdropping with technical means and looking-in operations; the National Informants Administrator, which functions at the judicial police's Directorate-General level under the supervision of the federal prosecutor (Article 47*decies* §2 CCP),[38] provides data on informants; the investigating judge (via the public prosecutors) provides data on anonymous witnesses and other investigation methods; the federal prosecutor provides data on anonymous witnesses, the protection of threatened witnesses, special investigation methods, and the other investigation methods.

The annual reports add that all information, except information regarding the wiretapping method, is provided via uniform forms and sent to the Criminal Policy Service of the Ministry of Justice.[39] For information regarding the wiretapping methods, the reports mention two ways of data gathering: first, an automatic transfer for users of the programme "Phoobs" developed by the federal police in view of standardized data collection with the different operators.[40] Phoobs creates an access file which is sent to the Federal Computer Crime Unit (FCCU) of the Federal Judicial Police (Directorate for Combating Economic and Financial Crime). Second, for non-Phoobs users, the FCCU requires an Excel spreadsheet to be completed by the investigating judge. The annual reports add that the FCCU also receives data from the federal police's unit that technically implements the wiretapping measure: the "Commissariat-general Special Units – National Technical and Tactical Support Unit – Central Technical Interception Facilities."

---

[37] The reports in implementation of Article 90*decies* CCP are available at the website of the Criminal Policy Service of the Ministry of Justice: http://www.dsb-spc.be/web/index.php?option=com_content&task=view&lang=nl&id=55

[38] Nationale Informantenbeerder (in Dutch), Gestionnaire des indicateurs (in French).

[39] Dienst voor het Strafrechtelijk Beleid (in Dutch), Service de la Politique Criminelle (in French).

[40] Belgian Institute for Postal Services and Telecommunications, "Synthese van de raadpleging door de raad van het bipt op verzoek van de minister voor ondernemen en vereenvoudigen van 29/04/2010 betreffende de praktische uitvoering van richtlijn 2006/24/EG van 15 maart 2006 (richtlijn betreffende de bewaring van gegevens)" (Summary regarding the implementation of the data retention directive 2006/24/EG of 15 March 2006), 2010, p. 14, available at http://www.bipt.be/public/files/nl/1259/3344_nl_2010-10-01_bipt-verslag_consultatie_data_retention-publieke_versie_v20101001_nl.pdf

Ultimately, the Criminal Policy Service of the Ministry of Justice processes the data and drafts the report for the Minister of Justice and, in copy, for the Board of Prosecutors General.

## 2. Current data

Below we provide, first, current data for law enforcement methods provided by the Ministry of Justice; second, current data for intelligence collection methods provided by the Belgian Standing Intelligence Agencies Review Committee (Standing Committee I); and, third, current data for government access provided by electronic communication companies.

### *a) Current data for law enforcement methods provided by the Ministry of Justice*

#### aa) Overview

As stated above (section I.B.1.), the Minister of Justice will report annually to the Parliament on the application of some but not all investigation methods. Article 90*decies* CCP requires reporting for only two electronic communications interception methods: the wiretapping measure (Article 90*ter* §1, 1° CCP) and the power to enter a house or a private place to enable eavesdropping with technical means (Article 90*ter* §1, 2° CCP). Hence, there are no reporting obligations for the collection of identification data of electronic communications (Article 46*bis* CCP), tracing of traffic data, and localization of electronic communications (Article 88*bis* CCP), and the network search (Article 88*ter* CCP). Although the reporting obligation also applies to looking-in operations (Article 46*quinquies* and 89*ter* CCP) and the special investigation methods observation (Article 47*sexies* CCP) and infiltration (Article 47*octies* CCP), the annual reports of the Minister of Justice – in implementation of Article 90*decies* CCP – do not specify the cases in which these measures were used in the context of the interception of electronic communications.

The annual reports of the Minister of Justice – in implementation of Article 90*decies* CCP – refer to the productive cooperation with the federal public prosecutor's office and the federal police, which resulted in accurate statistics on looking-in operations and the special investigation methods (observation and infiltration). But for the other investigation methods, the annual reports refer to the incomplete data collection and lacking coordination between the investigating judges and the public prosecutors. The annual reports therefore use the term indications rather than statistics. Furthermore, for the wiretapping measure, the annual reports mention the lack of general cooperation between the federal judicial police and local police services, such as failure to complete the evaluation forms and return them to the Ministry of Justice.

bb) Wiretapping

The first table below under this section gives an overview of the number of wiretapping measures performed by law enforcement agencies (Article 90*ter* §1, 1° CCP). The table also provides statistics regarding the object of the wiretapping measures:

The 2004 annual report contains figures in relation to the following categories for the wiretapping measure: 117 interceptions of landline numbers; 1390 interceptions of mobile numbers; nine interceptions of fax numbers; five interceptions of Internet (modems); and 136 non-specified interceptions. Regarding the eavesdropping measure, the 2004 annual report indicates that only one public prosecutor's office provided data, which more specifically noted two cases of eavesdropping. The 2005 annual report, however, provides more specific data on eavesdropping for 2004: 38 cases.

Since 2005, the annual reports have been using different categories: landline numbers, mobile numbers, IMEI numbers, and e-mails. As the 2011, 2012, and 2013 reports (for the years 2010, 2011 and 2012) only present a non-numerical marked line chart, the numbers provided below are an estimate based on the author's reading of these charts.

| **Wiretapping (Article 90*ter* §1, 1° CCP)** | | | | | |
|---|---|---|---|---|---|
| **Year** | **Number (#)** | **Object (#, estimate)** | | | |
| | | **Landline** | **GSM** | **IMEI** | **Mail** |
| 2005 | 2569# | 373# | 1660# | 536# | 0 |
| 2006 | 3036# | 511# | 2089# | 436# | 0 |
| 2007 | 3603# | 495# | 2473# | 632# | 3# |
| 2008 | 4881# | 686# | 3133# | 1062# | 0 |
| 2009[41] | 5653# | 114# | 2818# | 531# | 3# |
| 2010 | 6031# | 631# (estimate) | 4200# (estimate) | 1200# (estimate) | 0 |
| 2011 | 6671# | 621# (estimate) | 4800# (estimate) | 1250# (estimate) | 0 |
| 2012 | 6712# | 712# (estimate) | 4700# (estimate) | 1300# (estimate) | 0 |

[41] The total number exceeds the sum of the numbers provided per category. This could be due to an error in the 2009 annual report.

cc) Power to enter a house or a private place to enable eavesdropping with technical means

The second table concerns the power to enter a house or a private place in order to enable eavesdropping with technical means performed by law enforcement agencies (Article 90*ter* §1, 2° CCP): the reports of the Ministry of Justice do not indicate the number of measures executed but only the annual number of case files in which they were applied.

| **Power to enter a house or a private place to enable eavesdropping with technical means (Article 90*ter* §1, 2° CCP)** | |
|---|---|
| **Year** | **Number of case files in which measure applied (#)** |
| 2004 | 38# |
| 2005 | 29# |
| 2006 | 24# |
| 2007 | 24# |
| 2008 | 40# |
| 2009 | 40# |
| 2010 | 48# |
| 2011 | 54# |
| 2012 | 71# |

*b) Current data for intelligence collection methods provided by the Belgian Standing Intelligence Agencies Review Committee (Standing Committee I)*

aa) Overview

The next tables show the number of authorizations granted by the two intelligence agencies for the interception of electronic communications. The data are found in the activity reports of the Belgian Standing Intelligence Agencies Review Committee (Standing Committee I),[42] which has been providing data on the specific collection methods since 2010 and, since 2011, also for the exceptional collection methods. Thus, contrary to the lack of reporting obligations for law enforcement authorities regarding electronic communications methods other than the monitoring measure, the Standing Committee I provides statistics on *all* electronic communications interceptions collection methods.

---

[42] Belgian Standing Intelligence Agencies Review Committee (Standing Committee I), "Activity reports", available (in Dutch and French) at http://www.comiteri.be/index.php?option=com_content&view=article&id=40&Itemid=74&lang=EN. The Standing Committee I also produced three activity reports in English for the periods 2006-2007, 2008-2009, and 2010–2011.

The relevant specific collection methods are the collection of identification data of electronic communications (Article 18/2 §1, 4° and Article 18/7 of the Act of 30 November 1998), tracing of traffic data, and localization of electronic communications (Article 18/2 §1, 5 and Article 18/8 of the Act of 30 November 1998).

The relevant exceptional collection methods are the intrusion into a computer system (Article 18/2 §2, 6° and Article 18/16 of the Act of 30 November 1998) and wiretapping (Article 18/2 §2, 7° and Article 18/17 of the Act of 30 November 1998).

Of note is that the Standing Committee I did not provide any statistics regarding ministerial approval, and review by the Committee itself, of the interception of communications transmitted from abroad by the General Intelligence and Security Service of the Armed Forces (GISS) (Article 44*bis* of the Act of 30 November 1998).

Again, we only provide statistics that exclusively address the interception of electronic communications. The reason is, again, the lack of specification by the Ministry of Justice regarding cases in which other law enforcement measures (not explicitly created for the interception of electronic communications) were used in view of the interception of electronic communications.

The Standing Committee I provides separate statistics for the (civil) State Security[43] and the (military) General Intelligence and Security Service of the Armed Forces (GISS).[44] The 2010 activity report notes that the Standing Committee I could not could not give an indication of the number of measures actually implemented by the State Security, as the latter used its legal power to send these listings to the SIM commission only. The GISS, however, gave an indication of the results delivered by the various methods and, even more, showed the lack of implementation of a large number of methods authorized by the GISS in the reference period.[45]

### bb) Collection of identification data of electronic communications

The first table below refers to the specific collection method of collecting identification data of electronic communications (Article 18/2 §1, 4° and Article 18/7 of the Act of 30 November 1998). Of note is that, before 2013, the Standing Committee I did not show the number of measures but instead the annual number of case files in which they were applied.

In the 2012 activity report, the Standing Committee I explains that the decreasing frequency of this method, and also of the method of tracing traffic data of electronic communications, followed from its decision that these methods can no longer

---

[43] De Veiligheid van de Staat (VSSE, in Dutch), La Sûreté de l'Etat (VSSE, in French).

[44] De Algemene Dienst Inlichtingen en Veiligheid (ADIV, in Dutch), le Service général du Renseignement et de la Sécurité (SGRS, in French).

[45] See the 2010-2011 activity report (in English), pp. 68–69.

automatically result in the transfer of localization data (Article 18/2 §1, 5 and Article 18/8 of the Act of 30 November 1998).[46] In the 2013 activity report, the Standing Committee I confirmed an increasing number of localizations of electronic communications by both the State Security and the GISS.[47]

Although, since January 2013, identification data can no longer be authorized by the same authorization for the tracing of traffic data,[48] the decrease in identification data collection remained.

| Collection of identification data of electronic communications (Article 18/2 §1, 4° and Article 18/7 Act of 30 November 1998) | | |
|---|---|---|
| Year | Number of case files in which measure applied (#) | |
| | State Security | GISS |
| 2010 | 15# | 8# |
| 2011 | 355# | 23# |
| 2012 | 254# | 25# |
| 2013 | 243# (613# measures) | 16# (66# measures) |

cc) Tracing of traffic data, and localization of electronic communications

The next table concerns the specific collection method of tracing of traffic data of electronic communications, and localization of electronic communications (Article 18/2 §1, 5 and Article 18/8 of the Act of 30 November 1998).

| Tracing of traffic data, and localization of electronic communications (Article 18/2 §1, 5 and Article 18/8 Act of 30 November 1998) | | | | |
|---|---|---|---|---|
| Year | Tracing of traffic data (#) | | Localization (#) | |
| | State Security | GISS | State Security | GISS |
| 2010 | 30# | 7# | 6# | 7# |
| 2011 | 237# | 17# | 46# | 13# |
| 2012 | 147# | 30# | 176# | 4# |
| 2013 | 136# | 15# | 244# | 36# |

[46] See the 2012 activity report of the Standing Committee I, p. 49.

[47] See the 2013 activity report of the Standing Committee I, p. 69 (footnote 129), p. 71 (footnote 135), and p. 72.

[48] See the English 2010–2011 activity report of the Standing Committee I, p. 148; the 2012 activity report of the Standing Committee I, p. 49; and the 2013 activity report of the Standing Committee I, p. 68.

dd) Intrusion into a computer system

The next table concerns the specific collection method of intrusion into a computer system.

| Intrusion into a computer system (Article 18/2 §2, 6° and Article 18/16 Act of 30 November 1998) | | |
|---|---|---|
| Year | Number (#) | |
| | State Security | GISS |
| 2011 | 3# | 0 |
| 2012 | 10# | 2# |
| 2013 | 12# | 0 |

ee) Wiretapping

In the 2013 activity report, the Standing Committee I refers to an increasing number of wiretapping measures by both the State Security and the General Information and Security Service.[49]

| Wiretapping (Article 18/2 §2, 7° and Article 18/17 Act of 30 November 1998) | | |
|---|---|---|
| Year | Number (#) | |
| | State Security | GISS |
| 2011 | 11# | 2# |
| 2012 | 50# | 14# |
| 2013 | 81# | 17# |

*c) Current data provided by electronic communication companies*

aa) Vodafone

The 2014 law enforcement disclosure report of the telecommunications company Vodafone contains a legal annex providing an overview of law enforcement and intelligence powers in several countries, including Belgium.[50] In its analysis for Belgium, Vodafone refers to two demands for the disclosure of communication

---

[49] See the 2013 activity report, p. 72.

[50] Vodafone, "Law Enforcement Disclosure Report," 2014, available at http://www.vodafone.com/content/sustainabilityreport/2014/index/operating_responsibly/privacy_and_security/law_enforcement.html

data, saying that it has not implemented the technical requirements necessary to enable lawful interception and therefore did not receive any agency or authority demands for lawful interception assistance.[51]

### bb) Google

The following table shows the number of requests for user data that the technology company Google received, the number of users/accounts specified in the requests, and the percentage of request that Google complied with.[52]

| User data requests to Google | | | |
|---|---|---|---|
| **Period** | **Number (#)** | **Users/accounts (#)** | **Compliance rate (%)** |
| July to December 2009 | 67# | No data provided | No data provided |
| January to June 2010 | 71# | No data provided | No data provided |
| July to December 2010 | 85# | No data provided | 73% |
| January to June 2011 | 90# | 111# | 67% |
| July to December 2011 | 99# | 124# | 67% |
| January to June 2012 | 107# | 127# | 67% |
| July to December 2012 | 120# | 153# | 63% |
| January to June 2013 | 194# | 289# | 66% |
| July to December 2013 | 162# | 206# | 73% |
| January to June 2014 | 213# | 513# | 73% |
| July to December 2014 | 214# | 297# | 67% |

### cc) Microsoft

The following table shows the number of law enforcement requests made to the technology company Microsoft.[53] Like Google, Microsoft provides the number of requests for user data it has received, the number of users/accounts specified in the requests, and the percentage of requests it complied with. Unlike Google's trans-

---

[51] *Ibid.*, p. 71; see also Vodafone's "country-by-country disclosure of law enforcement assistance demands," available at http://www.vodafone.com/content/sustainabilityreport/2014/index/operating_responsibly/privacy_and_security/law_enforcement/country_by_country.html

[52] Google, "Transparency Reports," available via http://www.google.com/transparencyreport/?hl=en_US

[53] Microsoft, "Law Enforcement Requests Reports," available at https://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency/

parency reports, Microsoft breaks the compliance rate into three percentages: provided subscriber/transactional data; provided content data; or no data provided because no data were found. In addition, Microsoft provides a rejection rate showing the percentage of rejected requests for reasons of not meeting legal requirements. The law enforcement request reports cover requests for all Microsoft services, except for the 2012 report, which does not include the voice-call service Skype.

| User data requests to Microsoft | | | | | | |
|---|---|---|---|---|---|---|
| **Period** | **Number (#)** | **Rejection rate (#, %)** | **Users/ accounts (#)** | **Subscriber/ transactional data (#, %)** | **Content data (#, %)** | **No data found (#, %)** |
| January to December 2012 | 727# | 0% | 1140# | 629# 86,5% | 0% | 98# 13,5% |
| January to June 2013 | 500# | 0% | 784# | 406# 81,2% | 0% | 94# 18,8% |
| July to December 2013 | 378# | 12# 3,2% | 520# | 287# 75,9% | 0% | 79# 20,9% |
| January to June 2014 | 433# | 66# 1% | 922# | 360# 83,1% | 0% | 66# 15,2% |
| July to December 2014 | 481# | 17# 3,5% | 765# | 394# 81,9% | 0% | 70# 14,6% |

A brief comparison of the Google and Microsoft statistics shows that, prior to the latest Microsoft law enforcement request report (from 2012 till June 2014) the rejection rate was zero. The rejection rate of 3,5% for the period July to December 2014 is, however, still significantly lower than Google's rejection rate, which has remained stable at around 30% since 2010. Nevertheless, the number of requests to Microsoft has generally decreased, in contrast to the increasing number of requests to Google.

As the statistics of Microsoft show that no content data were provided to Belgian authorities, there is a high probability that Articles 46*bis* (identification data of electronic communications) and 88*bis* CCP (tracing of traffic data, and localization of electronic communications) were the legal bases for the data transfers.

#### dd) Twitter

The transparency reports of the social networking service Twitter show almost no information requests from Belgium.[54]

---

[54] Twitter, "Transparency reports," available via https://transparency.twitter.com/

| User data requests to Twitter | | | |
|---|---|---|---|
| **Period** | **Number (#)** | **Compliance (%)** | **Accounts (#)** |
| January to June 2012 | No data provided | No data provided | No data provided |
| July to December 2012 | 0 | Not applicable | Not applicable |
| January to June 2013 | 0 | Not applicable | Not applicable |
| July to December 2013 | 2# | 50% | 2# |
| January to June 2014 | 0 | Not applicable | Not applicable |
| July to December 2014 | 1# | 0% | 1# |

### ee) Facebook

The government request reports of the social media service Facebook show an increasing number of requests (like Google).[55] Whereas Google's compliance rate has remained stable at around 70%, Facebook's compliance rate has gradually decreased.

| User data requests to Facebook | | | |
|---|---|---|---|
| **Period** | **Number (#)** | **Compliance (%)** | **Users/accounts (#)** |
| January to June 2013 | 150# | 70% | 169# |
| July to December 2013 | 154# | 64,94% | 196# |
| January to June 2014 | 209# | 56,94% | 246# |
| July to December 2014 | 239# | 59% | 319# |

### ff) Verizon

The transparency reports of the US telecommunications provider Verizon do not provide the total number of requests received, nor compliance or rejection rates.[56]

Until the report for the second half of 2014, the transparency reports did not provide details regarding the number of requests for subscriber information and transactional information.

The 2013 transparency report specifies customer selectors (number of users/ accounts specified in the requests) for all requests complied with. The transparency

---

[55] Facebook, "Government requests reports," available via https://govtrequests.facebook.com/

[56] Verizon, "Transparency Reports," available via http://transparency.verizon.com/

report for the first half of 2014 breaks the customer selector rates into numbers for subscriber information and transactional information.

| User data requests to Verizon | | | | |
|---|---|---|---|---|
| Period | Number (#) | | Customer selectors (#) | |
| | Subscriber information | Transactional information | Subscriber information | Transactional information |
| 2013 | No data available | | 473# | |
| 1st half of 2014 | No data available | | 362# | 0 |
| 2nd half of 2014 | 173# | 0 | 193# | 0 |

# II. Principles of Telecommunication Interception in Constitutional and Criminal Procedure

## A. Constitutional Safeguards of Telecommunication

### 1. Areas of constitutional protection[57]

#### *a) Secrecy of telecommunication*

Private communications are protected by the constitutional right to privacy (Article 22 of the Belgian Constitution)[58] and the constitutional right of secrecy of communications (Article 29 of the Constitution).[59]

Article 22 of the Constitution reads as follows:

> Everyone has the right to the respect of his private and family life, except in the cases and conditions determined by the law.
>
> The laws, decrees, and rulings alluded to in Article 134 guarantee the protection of this right.

Article 29 of the Constitution reads as follows:

> The confidentiality of letters is inviolable.
>
> The law determines which nominated representatives can violate the confidentiality of letters entrusted to the postal service.

---

[57] The Belgian Constitution neither contains an explicit right to the confidentiality and integrity of information systems nor an explicit right to informational self-determination.

[58] An English version of the Constitution is available via www.legislationline.org

[59] See Paul De Hert and Serge Gutwirth, *Anthologie privacy/Anthologie de la vie privée* (Anthology of privacy), Academic and Scientific Publishers, 2013, p. 28, available at http://www.anthologieprivacy.be/sites/anthology/files/documents/anthologie-privacy-asp_0.pdf

*b) Core area of privacy*

Private communications are protected by the constitutional right to the inviolability of the home (Article 15 of the Constitution), the constitutional right to privacy (Article 22 of the Constitution), and the constitutional right of secrecy of communications (Article 29 of the Constitution, see II.A.1.a. above). The constitutional right to privacy protects against secret surveillance as well as monitoring and searching of computer data.

**2. Proportionality of access to data**

*a) Belgian Constitution*

The Belgian Constitution does not contain a constitutional principle of proportionality and necessity.

*b) Data Protection Act of 8 December 1992*

The Belgian Data Protection Act of 8 December 1992[60] includes the duty of observance of the principles of transparency and proportionality. Article 4 §1, 3° of the Act provides that personal data must be "adequate, relevant and not excessive in relation to the purposes for which it is collected or further processed." However, as mentioned below (see II.A.2.c.), the act contains certain exemptions, for instance in case of information gathering for police purposes.

*c) Act of 5 August 1992 on the Police Function*

Until 7 April 2014 (the date of entry into force of the Act of 18 March 2014),[61] Article 44/1 §1 of the Act of 5 August 1992 on the Police Function was phrased in general terms, allowing the police to gather information and intelligence on persons and groups that showed a concrete interest for the exercise of police functions. Professor De Hert and Vermeulen observed the general nature of this provision and its silence regarding systematic data collection.[62] The Act of 5 August 1992 on the

---

[60] Act of 8 December 1992 concerning the protection of privacy in relation to the processing of personal data, *Belgian Official Journal*, 18 March 1993, available at http://www.privacycommission.be/sites/privacycommission/files/documents/Privacy_Act_1992.pdf

[61] Act of 18 March 2014 regarding police information management and modifying the Act of 5 August 1992 on the Police Function, the Data Protection Act of 8 December 1992, and the Code of Criminal Procedure, *Belgian Official Journal*, 28 March 2014, entry into force on 7 April 2014.

[62] Paul De Hert and Mathias Vermeulen, "Toegang tot sociale media en controle door politie. Een eerste juridische verkenning vanuit mensenrechtelijk perspectief" (Access to

Police Function only mentioned the principle of proportionality and subsidiarity in relation to coercive police powers, more particularly in Article 37 which provides that any use of violence by the police services should be reasonable and in proportion to the pursued goals.

The Act of 18 March 2014 inserted a new Article 44/1 into the Act of 5 August 1992 on the Police Function, the first paragraph of which provides that the police services shall only process information and personal data insofar as sufficient, relevant, and not excessive in view of police purposes. Hence, this provision also applies to the powers for interception of electronic communications under (preventive) police law (see section I.A.2.b.): the general provision on crime detection and evidence gathering by the police (Article 8 CCP) and the specific provision on access by the police to publicly accessible places (Article 26 of the Act on the Police Function).

Furthermore, the Act of 18 March 2014 created a new Article 44/11/9, the fourth paragraph of which lays down a duty for the intelligence and security services, the Belgian Financial Intelligence Processing Unit (CTIF-CFI),[63] the Home Affairs Federal Public Service – Immigration Office,[64] and the prosecution and investigation services of the Federal Public Services Finance's General Administration Customs and Excise to transfer to the police services data and information that are processed within the framework of their functions and that are sufficient, relevant, and not excessive in view of police functions.

#### *d) Normal investigation methods*

Regarding the legal regime of criminal law, the principle of proportionality and necessity is found in relation to most, but not all, of the legal provisions for intercepting electronic communications. The principle is, first of all, foreseen for all normal investigation powers, except for the data seizure (Article 39*bis* CCP). The investigation methods to which the principle applies are thus the following: the collection of identification data of electronic communications (Article 46*bis* CCP), the tracing of traffic data, and localization of electronic communications (Article 88*bis* CCP), the network search (Article 88*ter* CCP), and the monitoring measure (Article 90*ter* §1 CCP).

---

social media and control by the police: a first legal exploration from the human rights perspective), *Panopticon*, 2012, vol. 33(2), p. (258) 261.

63 The CTIF-CFI is the Belgian preventive anti-money laundering and counter-terrorist financing system. De Cel voor Financiële Informatieverwerking (CFI, in Dutch), La Cellule de Traitement des Informations Financières (CTIF, in French).

64 Federale Overheidsdienst (FOD) Binnenlandse Zaken – Vreemdelingenzaken (in Dutch), Service Public Fédéral (SPF) Intérieur – Office des étrangers (in French).

*e) Special investigation methods and any other methods of investigation*

The Act of 6 January 2003 concerning special investigation methods and any other methods of investigation[65] introduced three *special investigation methods* and five *other investigation methods* into the CCP. Only the use of the special investigation methods is subject to the conditions of subsidiarity and proportionality.

The *special investigation methods* are observation (Article 47*sexies* CCP), infiltration (Article 47*octies* CCP), and the use of informants (Article 47*decie*s CCP). The two *special investigation methods* relevant for the interception of electronic communications are observation and infiltration.

The *other investigation methods* are the postponed intervention (Article 40*bis* CCP), the interception and opening of classical mail (Article 46*ter* CCP), the collection of data regarding bank accounts and bank transactions (Article 46*quater* CCP), looking-in operations (Articles 46*quinquies* and 89*ter* CCP), and the power to enter a house or a private place to enable eavesdropping with technical means (Article 90*ter* §1, 2° CCP). The two *other investigation methods* relevant for the interception of electronic communications are looking-in operations and the power to enter a house or a private place to enable eavesdropping with technical means.

*f) National collective agreement on the protection of the private lives of employees with respect to controls on electronic on-line communications data*

The national collective agreement on the protection of the private lives of employees with respect to controls on electronic on-line communications data, signed by Belgium's National Labour Council on 26 April 2002,[66] covers all on-line technologies, such as the Internet, e-mail, and Wireless Application Protocol (WAP), and has been drafted in sufficiently broad terms to also cover future developments. The agreement seeks to clarify and complement Article 8 of the ECHR, Article 22 of the Constitution (constitutional right to privacy), and the Act of 8 December 1992 on the protection of personal data. The obligations of the employer must respect the principle of proportionality: the controls impinging on an employee's private life must be kept to a minimum (Article 6); only data that are necessary for the control purpose may be collected or processed, i.e., as little possible data that affect the private life of the employee.

---

[65] Act of 6 January 2003 concerning special investigation methods and any other methods of investigation, *Belgian Official Journal*, 12 May 2003, entry into force on 22 May 2003.

[66] National Labour Council, "National collective agreement no. 81 of 26 April 2002 on the protection of the private lives of employees with respect to controls on electronic on-line communications data," 26 April 2002, available via www.cnt-nar.be. For a discussion of the agreement, see Paul De Hert, "C.A.O. no. 81 en advies no. 10/2000 over controle van Internet en e-mail" [Labour law: Soft law on e-mail and Internet practices], *Rechtskundig weekblad*, 2002-2003, vol. 66/33, 19 April 2003, pp. 1281–1294.

### 3. Consequences for the interception of telecommunication

The effective protection of the secrecy of telecommunications and the core area of privacy is guaranteed in several ways.

First, the right to privacy (Article 22 of the Constitution) applies to several spheres in the law of criminal procedure, including:[67]

- The secrecy of correspondence: Article 28*septies* §1 and Article 57 §1 CCP require the secrecy of correspondence on the part of everyone who contributes to the preliminary investigation respectively the investigation. Any breach of secrecy shall be punished in accordance with Article 458 of the Criminal Code. The following articles recall the principle of the secrecy of correspondence: Article 46*bis* CCP, Article 88*bis* CCP, Article 88*quater* CCP, Article 90*quater* CCP, Article 47*septies* CCP,[68] and Article 47*novies* CCP;[69]
- Wiretapping (Article 90*ter* CCP);
- The respect for professional secrecy: Article 90*sexies* §3, and Article 90*octies* CCP (see below, section II.A.4.b.).

Second, data collection by police services and law enforcement authorities is subject to control mechanisms (see also below on remedies against interception orders, section III.B.10.b.).

The Act of 18 March 2014[70] inserted a new Article 44/6 into the Act of 5 August 1992 on the Police Function, which foresees the establishment of a monitoring body for police information.[71]

The Courts in Chambers (a court of instruction in first instance)[72] and the Indictment Chamber (a court of instruction in appeal)[73] evaluate the legality of the

---

67 Brigitte Pesquié (revised by Yves Cartuyvels), "The Belgian system", in Mireille Delmas-Marty and John R. Spencer, *European Criminal Procedures*, Cambridge Studies in International and Comparative Law, Cambridge University Press, 2002, p. (81) 89.

68 Article 47*septies* CCP concerns the observation measure (Article 47*sexies* CCP).

69 Article 47*novies* CCP concerns the infiltration measure (Article 47*octies* CCP).

70 Act of 18 March 2014 regarding police information management and modifying the Act of 5 August 1992 on the Police Function, the Data Protection Act of 8 December 1992, and the Code of Criminal Procedure, *Belgian Official Journal*, 28 March 2014, entry into force on 7 April 2014.

71 Het Controleorgaan op de politionele informatie (in Dutch), L'Organe de contrôle de l'information policière (in French).

72 Raadkamer (in Dutch), Chambre du conseil (in French).

73 Kamer van Inbeschuldigingstelling (in Dutch), Chambres des mises en accusation (in French).

evidence collection during the investigation phase (Articles 131, 135 §2, and 235*bis* §6 CCP).[74]

Third, exclusionary rules demand the exclusion of illegally obtained evidence (see section IV.2. below).

Finally, criminal liability exists for the unlawful infringement of telecommunications (see section II.A.4.a. below).

### 4. Statutory protection of personal data

#### *a) Criminal liability for the unlawful infringement of telecommunication*[75]

This section only addresses criminal liability for unlawful infringements that directly target telecommunications.[76] Neither does it discuss *non-criminal* liability for the unlawful infringement of telecommunication.[77]

---

[74] Brigitte Pesquié (revised by Yves Cartuyvels), "The Belgian system", in Mireille Delmas-Marty and John R. Spencer, *European Criminal Procedures*, Cambridge Studies in International and Comparative Law, Cambridge University Press, 2002, (81) 87, 97.

[75] This section is partially based on the authors' earlier work: Paul De Hert and Gertjan Boulet, "Cybercrime report for Belgium," *International Review of Penal Law (RIDP / IRPL)*, 2013, issue 84, no. 1-2, pp. 12–59, available at http://www.penal.org/IMG/pdf/RIDP_2013_1_2_CD_Annexe.pdf, and *Electronic Review of the International Association of Penal* Law, 2013, http://www.penal.org/sites/default/files/files/RV-2.pdf; see also Paul De Hert and Frédéric Van Leeuw, "Cybercrime Legislation in Belgium," in Eric Dirix and Yves-Henri Leleu (eds.), *The Belgian reports at the Congress of Washington of the International Academy of Comparative Law*, Brussels, Bruylant, 2011, pp. 867–956, available at http://www.vub.ac.be/LSTS/pub/Dehert/389.pdf

[76] The following unlawful infringements do not necessarily directly target telecommunications: child pornography (Articles 383 and 283*bis* CC); grooming (Article 380*ter* §2 CC); stalking (Article 442*bis* CC for normal stalking, and Article 145 §3*bis* of the Act of 13 June 2005 on electronic communications for online stalking); defamation (libel, slander) (Article 443 CC); online gambling (see the Act of 10 January 2010 on gambling, *Belgian Official Journal*, 1 February 2010, entry into force on 1 January 2011); infringements of copyright (see the Act of 19 April 2014 inserting a book XI on 'intellectual property' into the Code of Economic Law, *Belgian Official Journal*, 12 June 2014, entry into force on 1 January 2014; the Act repealed the copyright Act of 30 June 1994, *Belgian Official Journal*, 27 July 1994, entry into force on 1 August 1994); the protection of databases and the rights of the producers of the databases (the Act of 19 April 2014 also repealed the Act of 31 August 1998 transposing the European directive from 11 March 1996 on the juridical protection of databases, *Belgian Official Journal*, 14 November 1998, entry into force on 14 November 1998); abuse registration of a domain name (see the Act of 15 December 2013 inserting book XII on " Law of the electronic economy" in the Code of Economic Law, *Belgian Official Journal*, 14 January 2014, entry into force on 31 May 2014. The Act repealed the Act of 26 June 2003 about the abuse of registration of a domain name, *Belgian Official Journal,* 9 September 2003, entry into force on 19 September 2003); provisions criminalizing racism and holocaust denial (see, for instance, the Act of 30 July 1981 to suppress certain acts inspired by racism and xenophobia, *Belgian Official Journal*, 8 August 1981, entry into force on 18 August 1981); and press crimes (judicial interpreta-

### aa) Traditional offenses in the Belgian Criminal Code

The Belgian Criminal Code (CC) traditionally criminalizes identity theft (Article 231), trespassing (Article 439), violations of professional secrecy (Article 458), and the secrecy of communications (Article 460).

### bb) The protection and interception of electronic communications: the Act of 30 June 1994

The Act of 30 June 1994 protecting privacy against the interception of communication and telecommunication[78] regulates both the protection and the interception of electronic communications. The Act introduced Article 314*bis* into the Belgian Criminal Code, which lays down the prohibition, applicable to everyone, of taking cognisance of the contents of electronic communications one does not participate in during the transfer of the electronic communications. A similar prohibition was introduced for public officials in Article 259*bis* CC. However, it should be noted that the monitoring exception in Article 90*ter* CCP provides an exception to the theoretical prohibition of the interception of electronic communications.

### cc) The Computer Crime Act of 28 November 2000

The Computer Crime Act of 28 November 2000[79] introduced new penal legislation concerning computer crimes in Belgium. The Act introduced new provisions into the Code of Criminal Law and the Code of Criminal Procedure. The law created the crime of computer forgery[80] (Article 210*bis*), computer fraud[81] (Arti-

---

tion of the right to freedom of expression and freedom of the press as shaped by Articles 19, 25, and 150 of the Constitution).

[77] Non-criminal liability for the unlawful infringement of telecommunication follows from infringements of the national collective agreement of 26 April 2002 on the protection of the private lives of employees with respect to controls on electronic on-line communications data (see section II.A.2. above). The collective agreement of 26 April 2002 was declared legally binding by Royal Decree of 12 June 2002 declaring legally binding the national collective agreement of 26 April 2002 on the protection of the private lives of employees with respect to controls on electronic on-line communications data, *Belgian Official Journal*, 29 June 2002, entry into force on 9 July 2002.

Article 189 of the Social Criminal Code of 6 June 2010 (*Belgian Official Journal*, 1 July 2010, entry into force on the same day) provides that infringements of generally legally binding, declared collective agreements shall be punished by a level 1 sanction, to be multiplied by the total number of employees involved. Article 100 of the Social Criminal Code provides that a level 1 sanction consists of an administrative fine of 10 to 100 euro.

[78] Act of 30 June 1994 protecting privacy against the interception of communication and telecommunication, *Belgian Official Journal*, 24 January 1995, entry into force on 3 February 1995.

[79] Wet inzake informaticacriminaliteit (in Dutch), Loi sur la criminalité informatique (in French), *Belgian Official Journal,* 3 February 2001, entry into force on 13 February 2002.

[80] Valsheid in informatica (in Dutch), faux en informatique (in French).

cle 540*quater*), hacking (Article 550*bis*), and sabotage of computer data/data and system interference[82] (Article 550*ter*).

dd) The Act of 13 June 2005 on electronic communications

Article 124 §§1 and 3 of the Act of 13 June 2005 on electronic communications protects the content of e-mails. Under Article 124 of the Act, the following actions are regarded as crimes unless the consent of all parties directly or indirectly involved has been given:

1. Intentionally taking note of the existence of signs, signals, writings, images, sounds, or data of any nature that originate from and are addressed to others;
2. Intentionally modifying or deleting this information by any technical means or identifying the other persons;
3. Intentionally taking note of telecommunication data that relate to other persons;
4. Disclosing, using in any way, modifying, or destroying the information, identification, and data set forth in 1, 2, and 3 above.

The Act of 13 June 2005 on electronic communications also contains a special penal provision in Article 145 §3, 1° that punishes anyone who carries out fraudulent electronic communications through a network of electronic communication. The provision can be used to prosecute hacking.

ee) The Belgian Data Protection Act of 8 December 1992

The Belgian Data Protection Act of 8 December 1992 imposes obligations on data controllers both in the public and in the private sector, although certain exemptions do exist, for instance in the case of information gathering for police purposes. The criminal provisions of the Act (Articles 37 to 39) provide a whole range of sanctions for the data controller who, if failing to meet his obligations, would jeopardize the confidentiality of data. These sanctions will undoubtedly apply to certain uses of personal data threatening the identity data of a person. Especially Article 39 of the Act is, in theory at least, a very suitable instrument to combat identity theft, hacking, secret surveillance, and websites with sensitive data hosted by individuals without permission, such as websites about suspected sex offenders.

> Article 39 of the Belgian Data Protection Act of 8 December 1992 punishes with a fine of one hundred to one hundred thousand francs
>
> 1) any controller, his representative in Belgium, appointee or agent who processes personal data in violation of the principles and requirements imposed in Article 4 §1 (finality principle, proportionality principle, etc.);

---

[81] Informaticabedrog (in Dutch), fraude informatique (in French).

[82] Informaticasabotage (in Dutch), sabotage de données informatiques (in French).

2) any controller, his representative in Belgium, appointee or agent who processes personal data in cases other than those permitted in Article 5 (consent, contract, legal ground);

3) any controller, his representative in Belgium, appointee or agent who processes personal data in violation of the Articles 6, 7 and 8 (regarding the so-called sensitive data);

4) any controller, his representative in Belgium, appointee or agent who has failed to comply with the obligations laid down in Article 9 (duty to inform the data subject);

5) any controller, his representative in Belgium, appointee or agent who fails to communicate the information referred to in Article 10 §1 within forty five days upon receipt of the request, or who knowingly communicates inaccurate or incomplete data;

6) any person who resorts to acts of violence or threat with the purpose to force another person to disclose information that is obtained through the exercise of the right as defined in Article 10 §1 or to give his consent for the processing of personal data relating to him;

7) any controller, his representative in Belgium, appointee or agent who starts, manages, continues to manage or terminates an automatic processing operation of personal data without compliance with the requirements of Prior notification to the National Data Protection Authority (Article 17);

8) any controller, his representative in Belgium, appointee or agent who communicates incomplete or inaccurate information in the notifications prescribed in Article 17;

[…]

10) any controller, his representative in Belgium, appointee or agent who, in violation of Article 19, refuses to communicate to the Commission the information relating to the non-automatic processing of personal data that are contained in a filing system or that are intended to be contained therein;

[…]

12) any person who transfers personal data, brings about or permits such transfer to a country outside the European Community that has been entered on the list referred to in Article 21 §2 in violation of the requirements of Article 22;

13) any person who prevents the Commission, its members or the experts who have been deployed by it from making the verifications referred to in Article 32.

### *b) Protection of professional secrets in criminal procedural law*

Article 89*ter* CCP (looking-in operations) provides a special rule for measures targeted at lawyers and doctors: In case the private place is a home, a part of a home, or the office of a lawyer of doctor, then the investigating judge (instead of the public prosecutor) has to authorize the measure.

The data retention Act of 29 May 2016 added a new paragraph 3 on professional secrecy to Article 88*bis* CCP (tracing of traffic data, and localization of electronic communications). The new paragraph 3 reflects Article 90*octies* CCP (wiretapping), and reads as follows:

The measure may only cover the electronic communications of a lawyer or a doctor, who themselves are suspected of having committed or participated in one of the criminal offenses referred to in the first paragraph, or if specific facts suggest that third parties

> suspected of having committed a criminal offense referred to in the first paragraph, use their electronic communications.
>
> The measure may not be implemented if, depending on the case, the president of the Bar or the representative of the provincial council of the order of physicians have not been informed of it. They will be informed by the investigating judge of what according to him shall be covered by professional secrecy. These data shall not be recorded in the official record.

Articles 90*sexies* and 90*octies* CCP provide special rules for wiretapping measures targeted at lawyers and doctors.

Article 90*sexies* §3 provides the following:

> The official record shall not include (tele-)communications covered by professional secrecy. Such (tele-)communications shall be kept at the Registry in a sealed envelope.[83] If it concerns persons referred to in Article 90octies, first paragraph, then shall be acted on the matter as provided in Article 90octies, second paragraph.

Article 90*octies* CCP reads as follows:

> The measure may only cover the premises used for business purposes, the domicile or the (tele-)communications means of a lawyer or a doctor, who themselves are suspected of having committed or participated in one of the criminal offenses referred to in article 90ter, or if specific facts suggest that third parties suspected of having committed a criminal offense referred to in Article 90ter, use their premises, domicile or (tele-) communications.
>
> The measure may not be implemented if, depending on the case, the president of the Bar or the representative of the provincial council of the order of physicians is not aware of it. They will be informed by the investigating judge of which according to him shall be considered as (tele-)communications covered by professional secrecy and not recorded in the official record under Article 90sexies, third paragraph.

### *c) Principle of "purpose limitation of personal data"*

Article 15, 1° of 5 August 1992 on the Police Function reads as follows:

> In the performance of their judicial police functions, the police have the task: 1° to detect the crimes, misdemeanours and contraventions, to gather evidence thereof, to notify the competent authorities thereof, to apprehend and arrest the perpetrators, to bring them at the disposal of the competent authorities, in the manner and forms provided by law;

Furthermore, as mentioned above (section II.A.2.c.), the Act of 18 March 2014 inserted a new Article 44/1 into the Act of 5 August 1992 on the Police Function, which provides that the police services shall only process information and personal data insofar as sufficient, relevant, and not excessive in view of police purposes.

Similarly, the data gathering practices of public prosecutors and investigating judges should be seen in light of their functions in conjunction with the prosecution

---

[83] The Act of 5 February 2016 added the specification that "[s]uch (tele-)communications shall be kept at the Registry in a sealed envelope." Act of 5 February 2016 regarding the modification of criminal law and criminal procedure and regarding diverse provisions on criminal policy, *Belgian Official Journal*, 19 February 2016, entry into force on 29 February 2016.

and investigation of criminal offenses. Article 28*bis* §1 CCP provides that "[t]he preliminary investigation is the whole of actions aimed at the detection of crimes, their perpetrators and evidence, and to collect the information relevant for the purposes of criminal proceedings." Article 55 CCP provides that "the investigation is the whole of action aimed at the detection of the perpetrators of crimes, to collect evidence and to take measures that allow the courts to pass informed judgments."

The Belgian Data Protection Act of 8 December 1992 imposes data protection obligations, including the principle of purpose limitation, on data controllers in the public and private sectors. However, as noted earlier (section II.A.2.c.), the Privacy Act contains some exemptions, e.g., for police purposes.

## B. Powers in the Code of Criminal Procedure

### 1. Requirement of (reasonable) clarity for powers in the law of criminal procedure

The *nullum crimen sine lege* principle also applies in the area of criminal procedure.[84] Article 12(2) of the Constitution reads as follows:

> The freedom of the individual is guaranteed.
>
> No one can be prosecuted except in the cases provided for by the law, and in the form prescribed by the law.
>
> Except in the case of a flagrant offence, no one can be arrested except on the strength of a reasoned judge's order, which must be served at the time of arrest or at the latest within twenty-four hours.

In his doctoral thesis on police powers and human rights, Goossens (former attorney-at-law, now member of the Standing Police Monitoring Committee[85]) uses the definition of the legality principle in the criminal procedural sense as proposed by Professor Traest:[86] a legal basis, which moreover should specify the competent authorities as well as the conditions under which the exercise of the investigation method may involve the infringement of human rights protected by the ECHR.[87]

---

[84] The principle also applies in the area of preventive police law. Article 1, §3 of the Act of 5 August 1992 on the Police Function provides that the police services shall only use coercive methods under the conditions determined by law.

[85] Vast Comité van toezicht op de politiediensten (*Comité P*, in Dutch), Comité permanent de contrôle des services de police (in French).

[86] Franky Goossens, *Politiebevoegdheden en mensenrechten in België. Rechtsvergelijkend en internationaal onderzoek* (Police powers and human rights in Belgium. Comparative and international research), doctoral thesis, Leuven, 2006, pp. 28–29, available at https://lirias.kuleuven.be/bitstream/1979/420/2/frankydoctoraat.pdf

[87] Philip Traest, "Rechts(on)zekerheid in materieel en formeel strafrecht en strafrechtelijk legaliteitsbeginsel" (Legal uncertainty in material and formal criminal law, and the

Goossens further embraces Professor Dupont's description of the legality principle as one of the most fundamental principles of criminal law and as a legal protective principle that finds its historic roots in a reaction against government arbitrariness in the criminal justice system of the ancien régime.[88]

The principle of strict interpretation of criminal law, and thereto related the prohibition of an analogous application of criminal law, is closely related to the principle of legality.[89] Legal doctrine traditionally discusses the prohibition of analogous application under criminal law rather than under the law of criminal procedure. In reality, we observe that law enforcement authorities apply the traditional monitoring measure (Article 90*ter* CCP) to electronic communications and thus allow the analogy between the wiretapping of traditional telecommunications and contemporary electronic communications (see below, section III.B.2.).[90] However, the annual reports of the Minister of Justice in implementation of Article 90*decies* CCP express the need for a modernization of the laws regarding wiretapping on the Internet (see below, section III.B.c.).[91]

### 2. Differentiation and classification of powers in the law of criminal procedure

The preliminary investigation methods in the Belgian law of criminal procedure are based on the distinction between the preliminary investigation/inquiry phase, under the responsibility of the public prosecutor, and the investigation/instruction phase, under the responsibility of the investigating judge who can also use coercive investigation methods.[92] Article 28*bis* §3 CCP provides that:

> [s]ubject to statutory exceptions, the preliminary investigation measures cannot involve coercive measure nor involve violation of individual rights and freedoms.

All reactive criminal law powers mentioned under section I.A.2.a. are principally reserved for the investigation phase, except for data seizure (Article 39*bis* CCP) and the collection of identification data of electronic communications (Article 46*bis* CCP).

---

principle of legality in criminal law), *Rechtskundig Weekblad*, 1993-1994, pp. (1190) 1192.

[88] Goossens, *op. cit.*, pp. 28, 30; Lieven Dupont, *Beginselen van strafrecht Deel 1* (Principles of criminal law vol. 1), Leuven, Acco, 2004, pp. 28, 29.

[89] Chris Van den Wyngaert, *Strafrecht, Strafprocesrecht & Internationaal Strafrecht in hoofdlijnen* (An Outline of Criminal Law, Criminal Procedural Law & International Criminal Law), Antwerp-Apeldoorn, Maklu, 2006, p. 80.

[90] Jan Kerkhofs and Philippe Van Linthout, *Cybercrime*, Brussels, Politeia, 2013, pp. 396, 244 and following.

[91] See above, section I.B.2.a. See, for instance, the 2013 report in implementation of Article 90*decies* CCP, pp. 18, 47, 48.

[92] Brigitte Pesquié (revised by Yves Cartuyvels), "The Belgian system", in Mireille Delmas-Marty and John R. Spencer, *European Criminal Procedures*, Cambridge Studies in International and Comparative Law, Cambridge University Press, 2002, (81) 87.

# III. Powers for Accessing Telecommunication Data in the Law of Criminal Procedure

## A. Overview

In this section, we briefly explain the legal provisions for intercepting electronic communications under (reactive) criminal law that are also listed under section I.A.2.a.

### 1. Normal investigation methods

Article 39*bis* CCP (data seizure) provides that the rules in the CCP on seizure apply to the copying, making inaccessible, and deleting of data stored in a computer system.

Article 46*bis* CCP (collection of identification data of electronic communications) empowers the public prosecutor to identify 1) the subscriber or the habitual user of an electronic communications service, 2) the electronic communication means used, and 3) the electronic communications services to which a particular person is a subscriber or that are habitually used by a particular person.

Article 88*bis* CCP (tracing of traffic data, and localization of electronic communications) empowers the investigating judge, and in specific cases the public prosecutor, to 1) trace traffic data of electronic communications means from which or to which electronic communications are or were made, 2) locate the origin or the destination of electronic communications.

Article 88*ter* CCP (the network search) empowers the investigating judge, when ordering a search of a computer system or a part thereof, to expand this search to a computer system or a part thereof at a place other than that at which the search takes place.

Article 90*ter* §1 CCP (wiretapping/monitoring) empowers the investigating judge, and in specific cases the public prosecutor, to wiretap, take cognizance of, and record private (tele-)communications during transmission.

### 2. Special investigation methods and any other methods of investigation

The Act of 6 January 2003 concerning special investigation methods and any other methods of investigation[93] introduced three *special investigation methods* and five *other investigation methods* into the CCP. The two *other investigation methods* relevant for the interception of electronic communications are looking-in opera-

---

[93] Act of 6 January 2003 concerning special investigation methods and any other methods of investigation, *Belgian Official Journal*, 12 May 2003, entry into force on 22 May 2003.

tions (Articles 46*quinquies* and 89*ter* CCP) and the power to enter a house or a private place to enable eavesdropping with technical means (Article 90*ter* §1, 2° CCP). The two *special investigation methods* relevant for the interception of electronic communications are observation (Article 47*sexies* CCP) and infiltration (Article 47*octies* CCP).

Articles 46*quinquies* and 89*ter* CCP (looking-in operations) empowers the public prosecutor to authorize police officers to enter a private place without the knowledge or consent of the owner.

Article 90*ter* §1, 2° CCP (the power to enter a house or a private place to enable eavesdropping with technical means) empowers the investigating judge, and in specific cases the public prosecutor, to directly monitor (eavesdropping), take cognizance of, or record private electronic communications with technical means.

Article 47*sexies* CCP (observation) empowers the public prosecutor and the investigating judge to order systematic observation by police officers of one or more persons; their presence or behavior; or of certain items, places, or events.

Article 47*octies* CCP (infiltration) empowers the public prosecutor and the investigating judge to authorize a police officer to maintain contact, under a false identity, with one or more persons for whom serious indications exist that they have committed or will commit either offenses within a criminal organization or offenses that are of a certain seriousness.

### 3. Cooperation with individuals and the private sector

For the execution of the above-mentioned investigation operations Belgian law enforcement agencies can cooperate with individuals and the private sector (Article 39*bis*, Article 46*bis*, Article 88*bis*, Article 88*quater*, Article 90*quater* §§2, 4 CCP).

Article 39*bis* §3 CCP (data seizure) allows public prosecutors to request an Internet Service Provider (ISP) to delete the domain name of a site that violates the law from their Domain Name Server (DNS).

Article 46*bis* CCP (collection of identification data of electronic communications) obliges operators of an electronic communications network and providers of an electronic communications service to provide identification data upon request of the public prosecutor.

Article 88*bis* CCP (tracing of traffic data, and localization of electronic communications) obliges operators of an electronic communications network and providers of an electronic communications service to provide traffic or localization data upon request of the public prosecutor.

Article 88*quater* CCP (network search) allows the public prosecutor to impose on certain individuals the obligation to cooperate during an investigation. These

individuals are persons of whom the investigating judge thinks that they have special capacities/knowledge concerning the computer system that is the object of an investigation or concerning services used to store, process, encrypt, or transfer data.

Article 90*quater* §2 CCP (wiretapping) obliges operators of an electronic communications network and providers of an electronic communications service to provide technical assistance to a data tapping measure upon request of the investigating judge.

Article 90*quater* §4 (wiretapping) echoes Article 88*quater* CCP.

Belgian law enforcement agencies can also cooperate with so-called closed user groups on the basis of Articles 122, 125, and 127 of the Electronic Communications Act[94] and with service providers acting as a mere conduit, catching and hosting on the basis of Articles XII.17 till XII.20 of the Code of Economic Law.[95]

Furthermore, in specific cases, judicial authorities can order a temporary surveillance period for Internet service providers acting as a mere conduit, catching and hosting (Article XII.20 of the Code of Economic Law).

### 4. Data retention

The general data retention (preservation) provision is Article 126 of the Electronic Communications Act,[96] which provides, among others, the providers that are subject to data retention obligations, the purposes of data retention, the obligations of the network and service providers, and the data retention periods. However, on 11 June 2015, the Belgian Constitutional Court invalidated article 126 of the Electronic Communications Act. A new Belgian data retention law of 29 May 2016 entered into force on 28 July 2016.

A Royal Decree of 19 September 2013 lists the types of data that are subject to data retention.[97]

Article 9 §7 of the Electronic Communications Act of 13 June 2005 provides that a specific Royal Decree shall address the matter of data retention for closed user

---

[94] Article 9 §7 of the Electronic Communications Act of 13 June 2005 provides that a specific Royal Decree shall address the matter of the cooperation between law enforcement agencies and closed user groups.

[95] Code of Economic Law of 28 February 2013, *Belgian Official Journal*, 29 March 2013, entry into force on 12 December 2013.

[96] As amended by the Belgian Communication Act of 30 July 2013 amending Articles 2, 126, and 145 of the Act of 13 June 2005 on electronic communications and Article 90*decies* of the Code of Criminal Procedure, *Belgian Official Journal*, 23 August 2013, entry into force on 2 September 2013.

[97] Royal Decree of 19 September 2013 regarding the execution of Article 126 of the Act of 13 June 2005 on electronic communications, *Belgian Official Journal*, 8 October 2013, entry into force on 19 September 2013.

groups. Federal Magistrate Jan Kerkhofs and Investigating Judge Philippe Van Linthout state that it could be said that Belgian providers of electronic communication services or networks with no notification duty are currently released from data retention obligations, taking into account the lack of a specific Royal Decree.[98] For the same reason, service providers that act as a mere conduit or provide caching and hosting activities under the Code of Economic Law are currently released from data retention obligations.

## B. Interception of Content Data

### 1. Statutory provision

Article 90*ter* CCP is the main provision in the law of criminal procedure dealing with the interception of the content of communications in transmission. Article 90*ter*, 1° CCP contains its core meaning:

> §1 The investigating judge may, in exceptional cases, when the investigation so requires, wiretap, take cognizance and record private (tele-)communications, during transmission, if there are serious indications that the offense for which he is seized is a criminal offense, as referred to in any of the provisions listed in §2, and if the other investigation methods are not sufficient to reveal the truth.
>
> In order to enable direct monitoring (eavesdropping), taking cognizance or recording of private (tele-)communications with technical means, the investigating judge may order, at any time, also without the knowledge or without the consent of either the resident or the owner or his rightful claimant, to enter a house or a private place.

### 2. Scope of application

#### *a) Object of interception*

Kerkhofs and Van Linthout say that the application of the wiretapping measure depends on three conditions pertaining to the nature of communications:

1) active communications;
2) private communications (see the text of Article 90*ter* CCP);
3) communications in transmission (see below, section III.B.2.).

The following facts show that electronic telecommunication falls under the material scope of the application of Article 90*ter* CCP.

First, we referred to the annual reports of the Minister of Justice in implementation of Article 90*decies* CCP, which provide statistics on the subjects of the wire-

---

[98] Jan Kerkhofs and Philippe Van Linthout, *Cybercrime*, Brussels, Politeia, 2013, p. 396.

tapping measures: landline numbers, mobile numbers, IMEI numbers, and e-mail (see section I.B.2.).

Second, the parliamentary preparatory works provide that the term (tele-)communications has a broad scope, as understood in its daily use: the term includes any linguistic expression, verbal or non-verbal, whether directly or from a physical distance, and irrespective of the number of participants. The term includes monologues, telegrams, telex, telefax, and electronic data transfers in computers and computer networks.[99]

Third, Kerkhofs and Van Linthout further specify that Article 90*ter* CCP covers the following forms of communication:[100]

- Classical telecommunications: analogous communication (voice and data) via landlines (landline numbers) and mobile communications;
- Pop-mail: e.g., Microsoft Outlook, Mozilla Thunderbird, Apple Mail;
- Webmail: e.g., Yahoo, Gmail, MSN, Hotmail;
- Voiceover IP (VoIP): e.g., Viber, Skype;
- Instant Messaging (IM) via
  - private chatrooms: e.g., Paltalk.com;
  - online gaming applications: e.g., World of Warcraft;
  - virtual gaming worlds: e.g., Second Lige;
  - mobile applications: e.g., WhatsApp, Google Talk, Blackberry Messenger.

It should be noted that IP data do not constitute private communications and therefore do not fall under the scope of Article 90*ter* CCP.

The available annual reports of the Minister of Justice as regards the implementation of Article 90*decies* CCP (until 2013) show no cases of wiretapping clouds or communications between two independent computer systems (e.g., between an automated machine and its computer-based automated control center, especially in the "Internet of things").

---

[99] Parliamentary preparatory works, regarding the legislative proposal protecting privacy against the interception of communication and telecommunication, Belgian Senate, 1992–1993, 1 September 1993, 843-1, p. 7, available at http://www.senate.be/lexdocs/S0539/S05390297.pdf; Parliamentary preparatory works, regarding the legislative proposal protecting privacy against the interception of communication and telecommunication, Belgian Senate, 1993–1994, 18 May 1994, 843-2, p. 38, available at http://www.senate.be/lexdocs/S0539/S05390364.pdf

[100] Jan Kerkhofs and Philippe Van Linthout, *Cybercrime*, Brussels, Politeia, 2013, pp. 279, 282, 295.

### *b) Temporal limits of telecommunication*

#### aa) Access to ongoing telecommunication

Article 90*ter* §1 CCP provides that the wiretapping measure only applies to (tele-)communications "during transmission."[101] For Kerkhofs and Van Linthout, the end of the transmission phase is the so-called "indicated necessary terminal," i.e., the place where an e-mail is deemed to arrive considering its nature and the e-mail configuration. They specify that, whereas the indicated necessary terminal of "pop-mail" is principally the user's own computer, the indicated necessary terminal of "webmail" is principally the user's online webmail account. Hence, pop-mail that arrives in an online web mailbox is still deemed to be in transmission, whereas webmail that arrives in an online web mailbox will be deemed to be out of transmission and therefore beyond the scope of the monitoring measure of Article 90*ter* CCP. In the latter case, law enforcement authorities will have to use a network search (Article 88*ter* CCP) to access the data. Hence, the use of a monitoring measure or a network search will depend on the specific e-mail configuration set by the user. In practice, however, pop-mail may *de facto* be configured as webmail, and vice versa. In case of doubt, law enforcement authorities issue a combined warrant: "90*ter* CCP versus 88*ter* CCP," or vice versa.

Kerkhofs and van Linthout also say that a wiretapping measure is possible in case of misuse of webmail, such as the sharing of one webmail account to exchange messages via e-mails stored in the draft folder. In this case, the transmission phase ends after login and reading of the draft e-mail by the recipient. Thus, in this case the end of the transmission phase seems conditioned by the "reading" of e-mails.

#### bb) Access after the end of telecommunication transmission

As said in the previous section, Article 90*ter* §1 CCP provides that the monitoring measure only applies to (tele-)communications *during transmission.* Hence, the monitoring measure does not apply when the respective data are stored before or after the transmission process.

### *c) Current matters of dispute*

A first current matter of dispute is the determination of the transmission phase. As previously said, for Kerkhofs and Van Linthout, pop-mail arriving in an online web mailbox is still deemed to be in transmission and therefore can be intercepted on the basis of Article 90*ter* CCP. Former attorney-at-law Dewandeleer confirmed

---

[101] Jan Kerkhofs and Philippe Van Linthout, *Cybercrime*, Brussels, Politeia, 2013, p. 288.

this view, which is based on a judgment of 4 December 2007 of the Correctional Court of Leuven.[102]

Arnou (attorney-at-law), however, says that the wiretapping measure is not possible for e-mails stored on the server of the service provider.[103] His reasoning echoes the parliamentary preparatory works of 1998 modifying Act of 30 June 1994 protecting privacy against the interception of communication and telecommunication, which state that e-mails stored on the server of a service provider do not enjoy the privacy protection against the interception of (tele-)communications (Article 314*bis* and Article 259*bis* CC, see section II.A.4. above) but are possibly protected by other criminal laws. Therefore, the parliamentary preparatory works say such e-mails cannot be intercepted on the basis of Article 90*ter* CC but on the basis of other investigation methods, such as the powers of search and seizure (Article 39*bis* CCP) and the network search (Article 88*ter* CCP).[104]

The foregoing shows that constitutional reasoning regarding the scope of privacy and criminal law protection, such as the protection against the interception of (tele-)communications offered by Article 314*bis* and Article 259*bis* CC, could influence the discussions regarding the scope of the wiretapping measure.

An additional current matter of dispute is the difficulty of determining the transmission phase on social media, considering for instance the potential impact of status messages on Facebook. Kerkhofs and Van Linthout have therefore proposed a rewriting of the laws on wiretapping.[105] As said earlier, the annual reports of the Minister of Justice in implementation of Article 90*decies* CCP also express the need for a modernization of the laws regarding wiretapping on the Internet.[106]

---

[102] Dirk Dewandeleer, "De kennisname van e-mails 'tijdens de overbrenging ervan', een verduidelijking van het telecommunicatiegeheim" (Taking knowledge of e-mails during the transmission phase. A clarification of the secrecy of telecommunications), annotation to the judgment of the Correctional Court of Leuven, 4 December 2007), *Tijdschrift voor Strafrecht*, 2008, vol. 3, p. [226] 226.

[103] Luc Arnou, "Afluisteren tijdens het gerechtelijk onderzoek" (Wiretapping during the investigation); in Commentaar Strafrecht en strafvordering (Commentary criminal law and criminal procedural law), Gent, Kluwer, 2008, vol. 59, pp. 13–14, no. 12.

[104] Parliamentary preparatory works, modifying the Act of 30 June 1994 protecting privacy against the interception of communication and telecommunication, Belgian Chamber of Parliaments, 1996-1997, 29 May 1998, no. 49K1075/017, p. 10, available at http://www.dekamer.be/FLWB/PDF/49/1075/49K1075017.pdf

[105] Jan Kerkhofs and Philippe Van Linthout, *Cybercrime*, Brussels, Politeia, 2013, p. 246.

[106] See I.B.2.a. above. See, for instance, the 2013 annual report of the Minister of Justice in implementation of Article 90*decies* CCP, pp. 18, 47, 48.

### 3. Special protection of confidential communication content

#### *a) Privileged communication*

##### aa) Professional secrets

(1) Conditional protection of lawyer's and doctor's secrets against the monitoring measure: in case of suspicion only and after notification of the Bar and the order of physicians

Article 90*octies* §1 and §2, 1° read as follows:

> The monitoring measure may only cover the premises used for business purposes, the domicile or the (tele-)communications means of a lawyer or a doctor, who themselves are suspected of having committed or participated in one of the criminal offenses referred to in article 90ter, or if specific facts suggest that third parties suspected of having committed a criminal offense referred to in Article 90ter, use their premises, domicile or (tele-)communications.
>
> The monitoring measure may not be implemented if, depending on the case, the president of the Bar or the representative of the provincial council of the order of physicians is not aware of it. […]

Accordingly, the conditions of "suspicion" and "notification of the Bar and the order of physicians" only hold for a monitoring measure that covers premises used for business purposes, the domicile, or the (tele-)communications means of a lawyer or a doctor.

Arnou and public prosecutor Freyne hold that compliance with the notification duty follows from a written notification or confirmation of an oral notification in an official record.[107] Although notification of the Bar and the order of physicians is not prescribed under sanction of nullity (see below on the exclusionary rules, section IV.2.), the parliamentary preparatory works underline that the public order nature of this provision implies that failure to do so will entail the nullity of the monitoring measure.[108] As said below, in a judgment of 18 February 2003,[109] the Supreme Court held that the rights of the defense may justify access by the defense to the documents resulting from a nullified investigation method. In fact, these

---

[107] Luc Arnou, "Afluisteren tijdens het gerechtelijk onderzoek" (Wiretapping during the investigation); in Commentaar Strafrecht en strafvordering (Commentary criminal law and criminal procedural law), Gent, Kluwer, 2008, vol. 59, p. 36, no. 33; Thierry Freyne, "De bewaking van privécommunicatie en –telecommunicatie in strafonderzoeken: een stand van zaken" (The monitoring of private communications and telecommunications in criminal proceedings: a state of affairs), *Tijdschrift voor Strafrecht*, 2008, vol. 3, p. 177, no. 33.

[108] Parliamentary preparatory works, regarding the legislative proposal protecting privacy against the interception of communication and telecommunication, Belgian Senate, 1993–1994, 18 May 1994, no. 843-2, p. 189, available at http://www.senate.be/lexdocs/S0539/S05390364.pdf

[109] Supreme Court, 18 February 2003, P.02.0913.N.

documents are not deleted but kept at the Registry in a sealed envelope (Article 235*bis* §6 CCP).

(2) Unconditional protection of professional secrets against inclusion in official records

Article 90*sexies* §3, 1° CCP protects *all* possible professional secrets, such as communication between an attorney-at-law and a client, a medical practitioner and a patient, journalists' communications, communication under the law regulating financial and banking secrecy, etc. The provision provides that "[t]he official records shall not include (tele-)communications covered by professional secrecy."

Article 90*sexies* §3, 2° CCP, read in conjunction with Article 90*octies* §2, 2° CCP, provides additional protection for lawyers and doctors:

> Article 90sexies §3 CCP: If it concerns persons referred to in Article 90octies, first paragraph, then shall be acted on the matter as provided in Article 90octies, second paragraph.
>
> Article 90octies §2, 2° CCP: They [the president of the Bar or the representative of the provincial council of the order of physicians] will be informed by the investigating judge of what according to him shall be considered as (tele-)communications covered by professional secrecy and shall not be recorded in the official record under Article 90sexies, third paragraph.

Although the recordings protected by professional secrecy are not recorded in the official record, they are kept at the Registry in a closed and sealed envelope on the basis of Article 90*septies* §3 CCP.[110] Article 90*septies* §§6–8 CCP provides cases in which the investigating judge or the court *may* upon request allow access to the whole or parts of the recordings deposited at the Registry:[111]

> The defendant, the accused, the civil party, the civilly liable party or their counsel shall receive upon request a copy of all the records of the (tele-)communications of which relevantly deemed parts were transcribed and recorded in an official record to which they have access.
>
> The judge shall decide on the request of the defendant, the accused, the civil party or their counsel, to consult the whole or parts of the other recordings deposited at the Registry, and transcripts that are not recorded in an official record, as well as on their request to transcribe additional parts of the recordings.

---

[110] Thierry Freyne, "De bewaking van privécommunicatie en -telecommunicatie in strafonderzoeken: een stand van zaken" (The monitoring of private communications and telecommunications in criminal proceedings: a state of affairs), *Tijdschrift voor Strafrecht,* 2008, vol. 3, p. 177, no. 30.

[111] The Act of 5 February 2016 added a new (fifth) paragraph to Article 90*septies* CCP, laying down a right for some parties to access a copy of all the records of the (tele-) communications of which relevantly deemed parts were transcribed and recorded in an official record to which they have access. Act of 5 February 2016 regarding the modification of criminal law and criminal procedure and regarding diverse provisions on criminal policy, *Belgian Official Journal*, 19 February 2016, entry into force on 29 February 2016.

The request addressed to the investigating judge, is treated in accordance with Article 61quinquies. The investigating judge may also refuse this request for reasons connected with the protection of other individual rights or interests.

bb) Protection of the core area of privacy

Article 90*ter* CCP provides no additional protection for the core area of privacy.

*b) Responsibility for ensuring protection*

The articles discussed in the previous section show that the responsibility for ensuring the protection of professional secrets lies with the investigating judge, thus the magistrate that issues the warrant.

The investigating judge, however, has no complete discretion to determine the stage of the interception phase in which, and the way in which, these privileges have to be conducted. It is recalled, first, that, according to Article 90*octies* §2, 1° CCP, a monitoring measure in respect of the premises used for business purposes, the domicile, or the (tele-)communications means of a lawyer or a doctor may only be implemented *after* notification, depending on the case, of the president of the Bar or the representative of the provincial council of the order of physicians. Second, according to Article 90*octies* §2, 2° CCP, the investigating judge shall inform the president of the Bar or the representative of the provincial council of the order of physicians of what, according to him, shall be considered (tele-)communications covered by professional secrecy and thus not be recorded in the official record under Article 90*sexies*, third paragraph.

However, the investigating judge seems to have more discretion as regards the analysis of the captured information. In fact, the president of the Bar or the representative of the provincial council of the order of physicians does not have the right to be consulted prior to assessment by the investigating judge of what, according to him, shall be considered (tele-)communications covered by professional secrecy. Neither do they have any right of co-decision or contradiction.[112]

## 4. Execution of telecommunication interception

*a) Execution by the authorities with or without the help of third parties*

As said, the monitoring measure is laid down in Article 90*ter*, 1° and 2° CCP. A literal reading of the law shows that the Belgian law enforcement authorities do not necessarily need to cooperate with third parties. For instance, law enforcement

---

[112] Raf Verstraeten, *Handboek strafvordering* (Manual on criminal procedure), Antwerp, Maklu, 2007, p. 472, no. 948.

authorities can use their own technical equipment to execute an eavesdropping measure (see below III.B.4.b.).

Article 90*quater* §§2, 4 CCP lays down the cooperation duties for individuals and the private sector.

Article 90*quater* §2, 1° CCP reads as follows:

> §2. If the measure involves an operation on a communications network, then is the operator of this network or the provider of the telecommunications service obliged to provide technical cooperation, if the investigating judge requests so directly or via a by the King designated police service.[113] […]

Article 90*quater* §4, 1-2° CCP reads as follows:

> The investigating judge can order, directly or via a by the King designated police service, persons of whom he thinks that they have special knowledge of the telecommunications service subject to the monitoring measure, or of services used to protect or encrypt data that are stored, processed, encrypted or transferred via a computer system, to provide information on the operation of the system and on the way to get access to the content of the telecommunication, that is or has been transferred, in an understandable format.
>
> He can order persons to make the content of telecommunications accessible in the format requested by him. These persons are obliged to comply with the order, to the extent of their capabilities. […]

Media reports have also alleged direct access by Belgian law enforcement agencies to the servers of operators and service providers.[114] Vodafone's online presentation of its 2014 law enforcement disclosure report confirms this practice but does not specify which countries allow such direct access:

> However, in a small number of countries the law dictates that specific agencies and authorities must have direct access to an operator's network, bypassing any form of operational control over lawful interception on the part of the operator. In those countries, Vodafone will not receive any form of demand for lawful interception access as the relevant agencies and authorities already have permanent access to customer communications via their own direct link.[115]

In our view, it should be kept in mind that the monitoring measure in Article 90*ter* CCP cannot be applied to proactive investigations, and that the modalities

---

[113] The Act of 5 February 2016 amended Article 90*quater* §2, 1° CCP and Article 90*quater* §4, 1-2° CCP, and added the possibility for the investigating judge to request technical cooperation via a police service appointed by the King. Act of 5 February 2016 regarding the modification of criminal law and criminal procedure and regarding diverse provisions on criminal policy, *Belgian Official Journal*, 19 February 2016, entry into force on 29 February 2016.

[114] Cf. The Washington Post, "Do France and Belgium have direct wiretap access to telecom switches?," 7 June 2014, available at http://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/06/07/do-france-and-belgium-have-direct-wiretap-access-to-telecom-switches/

[115] Vodafone, "Law Enforcement Disclosure Report," via https://www.vodafone.com/content/sustainabilityreport/2014/index/operating_responsibly/privacy_and_security/law_enforcement.html

of the cooperation duties under Article 90*quater* §2 and §4 CCP are laid down in the Royal Decree of 9 January 2003 regarding the legal duty to cooperate with judicial requests regarding electronic communications.[116] The Royal Decree installs a Coordination Cell Justice responsible for handling the information requests by Belgian legal authorities. According to Article 4 of the Royal Decree, the Coordination Cell Justice shall transfer the data in real time after receipt of the warrant in Article 90*ter* §1 or §5 CCP. Hence, direct access by law enforcement to the servers of operators and service providers seems questionable, considering the installation of the Coordination Cell Justice for cooperation with law enforcement.

In this regard, the following standard set by the European Telecommunications Standards Institute may also be considered:[117]

> [T]he result of interception shall only be transmitted to the Law Enforcement Monitoring Facility [LEMF] as indicated in the lawful authorization when proof of the authority to receive of the LEMF, and proof of the authority to send of the interface, has been furnished;

*b) Accompanying powers for the execution of interception*

Article 90*ter* §2 CCP allows clandestine access to a house in order to install equipment to carry out the eavesdropping measure:

> In order to enable direct monitoring (eavesdropping), taking cognizance or recording of private (tele-)communications with technical means, the investigating judge may order, at any time, also without the knowledge or without the consent of either the resident or the owner or his rightful claimant, to enter a house or a private place.

Article 90*ter* CCP does not explain the meaning of the term technical means as to whether or not it can also include technical means falling under the definition of technical means for a looking-in operation and observation (see below, section III.D.1.). Furthermore, the parliamentary preparatory works deliberately give no definition of technical means under Article 259*bis* CC (protection of telecommunications) because any such definition would risk beoming outdated due to techno-

---

[116] Royal Decree of 9 January 2003 regarding the legal duty to cooperate with judicial requests regarding electronic communications, *Belgian Official Journal*, 10 February 2003, entry into force on 10 May 2003; The Royal Decree of 9 January 2003 was amended by the Royal Decree of 8 February 2011: Royal Decree of 8 February 2011 modifying Royal Decree of 9 January 2003 regarding the execution of the Royal Decree of 9 January 2003 regarding the execution of Article 46*bis* §2, paragraph 1, 88*bis* §2, paragraphs 1 and 3 and 90*quater* §2 paragraph 3 CCP and of Article 109*ter* E §2 of the Act of 21 March 1991 on the reform of certain economic public enterprises, *Belgian Official Journal*, 23 February 2011, entry into force on 5 March 2011.

[117] European Telecommunications Standards Institute, "TS 101-331 Lawful Interception (LI); Requirements of Law Enforcement Agencies," V1.1.1 (2001-08), 4.7.g, available at http://www.etsi.org/deliver/etsi_TS/101300_101399/101331/01.01.01_60/ts_101331v010101p.pdf

logical developments.[118] However, the parliamentary preparatory works prohibit the intrusion into a computer system (hacking) for the monitoring measure of Article 90*ter* CCP.[119]

Professor De Valkeneer, who is also a Prosecutor General, explains that technical means under Article 90*ter* CCP can include micro-spies, key-loggers, and parabolic microphones outside a home or private place.[120] As said earlier (section I.A.2.), the general wiretapping measure under Article 90*ter* §1, 1° CCP includes direct monitoring/eavesdropping and can therefore also be executed with technical means outside a home or a private place. The eavesdropping measure under Article 90*ter* §1, 2° CCP, however, concerns the power to enter a house or a private place in order to enable eavesdropping with technical means.

Dr. De Wolf asks himself whether viruses could also be used for the monitoring measure.[121]

### 5. Duties of telecommunication service providers to cooperate

#### *a) Possible addressees of duties of cooperation*

As said above (section III.B.5.a.), the cooperation duties for individuals and the private sector, provided in Article 90*quater* §§2, 4 CCP apply to the operators of a communications network, the provider of a telecommunications service, and any persons of whom the investigating judge thinks that they have special knowledge of the telecommunications service subject to the monitoring measure. They also apply to the operators/providers of services used to protect or encrypt data that are stored, processed, encrypted, or transferred via a computer system.

Hence, the personal scope of application of the cooperation duty is quite broad and includes infrastructure providers working at the IP-transport level (operators of a telecommunications network), Internet Access Providers (IAPs) and Internet Service Providers (ISPs), such as social media providers and cloud computing service providers.

---

[118] Parliamentary preparatory works, regarding the legislative proposal protecting privacy against the interception of communication and telecommunication, Belgian Senate, 1992-1993, 1 September 1993, no. 843-1, p. 6, available at http://www.senate.be/lexdocs/S0539/S05390297.pdf

[119] Parliamentary preparatory works, regarding the legislative proposal protecting privacy against the interception of communication and telecommunication, Belgian Senate, 1992-1993, 1 September 1993, no. 843-1, p. 11, available at http://www.senate.be/lexdocs/S0539/S05390297.pdf

[120] Christian De Valkeneer, *Manuel de l'enquête pénale* (Manual on criminal investigation), Brussels, Larcier, 2006, p. 334.

[121] Daniel De Wolf, "Rapport Belge" (Belgian report on criminal procedure), *Electronic Review of the International Association of Penal Law*, 2014, p. 23, available at http://www.penal.org/sites/default/files/files/RA%20-%203.pdf

Of note in this regard is a judgment of the Belgian Supreme Court of 18 January 2011 (see section III.C.1.dd.), in which the court gave an autonomous (broad) interpretation of the term "electronic communications provider" mentioned in Article 46*bis* CCP (the collection of identification data of electronic communications).

*b) Content of duties to cooperate*

Article 90*quater* §§2, 4 CCP lays down the cooperation duties for individuals and the private sector.

Article 90*quater* §2, 1° CCP reads as follows:

> §2. If the measure involves an operation on a communications network, then is the operator of this network or the provider of the telecommunications service obliged to provide technical cooperation, if the investigating judge requests so directly or via a by the King designated police service.[122] […]

Article 90*quater* §4, 1° and 2° CCP reads as follows:

> §4 The investigating judge can order, directly or via a by the King designated police service, persons of whom he thinks that they have special knowledge of the telecommunications service subject to the monitoring measure, or of services used to protect or encrypt data that are stored, processed, encrypted or transferred via a computer system, to provide information on the operation of the system and on the way to get access to the content of the telecommunication, that is or has been transferred, in an understandable format.
>
> He can order persons to make the content of telecommunications accessible in the format requested by him. These persons are obliged to comply with the order, to the extent of their capabilities.

The modalities of the cooperation duties under Article 90*quater* §§2, 4 CCP are laid down in the Royal Decree of 9 January 2003 regarding the legal duty to cooperate with judicial requests regarding electronic communications.[123] The Royal Decree installs a Coordination Cell Justice responsible for handling the information requests from Belgian legal authorities.

---

[122] The Act of 5 February 2016 amended Article 90*quater* §2, 1° CCP and Article 90*quater* §4, 1° and 2° CCP, and added the possibility for the investigating judge to request technical cooperation via a by the King appointed police service. Act of 5 February 2016 regarding the modification of criminal law and criminal procedure and regarding diverse provisions on criminal policy, *Belgian Official Journal*, 19 February 2016, entry into force on 29 February 2016.

[123] Royal Decree of 9 January 2003 regarding the legal duty to cooperate with judicial requests regarding electronic communications, *Belgian Official Journal*, 10 February 2003; The Royal Decree of 9 January 2003 was amended by the Royal Decree of 8 February 2011 modifying the Royal Decree of 9 January 2003 regarding the execution of the Royal Decree of 9 January 2003 regarding the execution of Article 46*bis* §2, paragraph 1, 88*bis* §2, paragraph 1 and 3 and 90*quater* §2 paragraph 3 CCP and of Article 109*ter* E §2 of the Act of 21 March 1991 on the reform of certain economic public enterprises, *Belgian Official Journal*, 23 February 2011, entry into force on 5 March 2011.

A circular of the Board of Prosecutors General of 17 December 2009 explains the criminal policy regarding violations of the cooperation duties under Article 46*bis* §2 CCP (the collection of identification data of electronic communications), Article 88*bis* §2 CCP (tracing of traffic data, and localization of electronic communications), and Article 90*quater* §2 CCP.[124]

*c) Duties to provide technical and organizational infrastructure*

aa) Obligated parties

Article 1, 5° of the Royal Decree of 9 January 2003 regarding the legal duty to cooperate with judicial requests regarding electronic communications defines its personal scope of application in terms of the "Internet sector," i.e., the entirety of operators of electronic communications networks and providers of electronic communications services.

bb) Individual technical obligations

Article 6 §3 of the Royal Decree of 9 January 2003 regarding the legal duty to cooperate with judicial requests regarding electronic communications provides that the technical requirements for the data transfer need to comply with the following updated standards and reports of the European Telecommunications Standards Institute:

1) TS 101-331: Lawful Interception (LI); Requirements of Law Enforcement Agencies;
2) TS 101-671: Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic;
3) TS 101-909-20-1: AT Digital. Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 20: Lawful Interception; Sub-part 1: CMS based Voice Telephony Services;
4) TS 101-909-20-2 AT Digital. Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 20: Lawful Interception; Sub-part 2: Streamed multimedia services;
5) TR 101-943: Lawful Interception (LI); Concepts of Interception in a Generic Network Architecture;

---

[124] Board of Prosecutors General, "Telecommunicatierichtlijn inzake het opsporings- en vervolgingsbeleid betreffende inbreuken op de medewerkingsverplichtingen vervat in de artikelen 46bis § 2, 88bis § 2 en 90quater § 2 van het wetboek van strafvordering" (Telecommunications Circular regarding the investigation and prosecution of violations of the cooperation duties under Articles 46*bis* §2, 88*bis* §2 and 90*quater* §2 CCP), COL 14/2009, 17 December 2009, available (in Dutch and French) at http://www.om-mp.be/omzendbrief/4420834/col_14-2009_dd__17_12_2009.html

6) TR 101-944: Lawful Interception (LI); Issues on IP Interception;
7) TR 102-053: Lawful Interception (LI); Notes on ISDN LI functionality;
8) TS 102-232: Lawful Interception (LI); Handover Specification for IP Delivery;
9) TS 102-233: Service-specific details for e-mail services;
10) TS 102-234: Lawful Interception (LI); Service-specific details for internet access services;
11) TS 102-815: Lawful Interception (LI); Service-specific details for Layer 2 Lawful Interception;
12) TS 133-10: Universal Mobile Telecommunication System (UMTS); "Lawful interception requirements (3GPP TS 33.106 version 5.1.0 Release 5) [3GPP SA3];
13) TS 133-107: Universal Mobile Telecommunication System (UMTS); 3G security; Lawful interception architecture and functions (3GPP TS 33.107 version 5.5.0 Release 5) [3GPP SA3];
14) TS 133-108: Universal Mobile Telecommunications System (UMTS); 3G security; Handover interface for Lawful interception (LI) (3GPP TS 33.108 version 5.4.0 Release 5) [3GPP SA3];
15) ES 201-158: Lawful Interception (LI); Requirements for Network Functions;
16) ES 201-671: Lawful Interception (LI): Handover Interface for the Lawful Interception of Telecommunications traffic;
17) Digital cellular telecommunications system (Phase 2+); Lawful interception requirements for GSM (GSM 01.33 version 8.0.0 Release 1999) [TC SMG] TR 101 514;
18) Digital cellular telecommunications system (Phase 2+); Lawful interception – Stage 1 (GSM 02.33 version 8.0.1 Release 1999) [TC SMG] TR 101 507;
19) Digital cellular telecommunications system (Phase 2+); Lawful interception – Stage 1 (3GPP TS 43.033 version 5.0.0 Release 5) [3GPP SA3] TR 143 033;
20) Digital cellular telecommunications system (Phase 2+); Lawful interception – Stage 1 (3GPP TS 42.033 version 5.0.0 Release 5) [3GPP SA3] TR 142 033;
21) Digital cellular telecommunications system (Phase 2+); Lawful interception requirements for GSM (3GPP TR 41.033 version 5.0.0 Release 5) [3GPP SA3] TR 141 033;
22) Digital cellular telecommunications system (Phase 2+) (GSM); Lawful interception – Stage 2 (3GPP TS 03.33 version 8.1.0 Release 1999) [3GPP SA3] TS 101 509.

cc) Organizational obligations

Article 2 of the Royal Decree of 9 January 2003 regarding the legal duty to cooperate with judicial requests regarding electronic communications requests operators of electronic communications networks and providers of electronic communications services to install a Coordination Cell Justice, individually or jointly, to handle the information requests from Belgian legal authorities.

*d) Security requirements for data transfers by communication service providers*

The following, rather broad, norms exist concerning the technical aspects of the transfer of intercepted data.

aa) Format

Article 90*quater* §4 CCP provides that the investigating judge can order persons to make the content of telecommunications accessible in the format requested by him, to the extent of their capabilities.

Article 10*bis*, 1° of the Royal Decree of 9 January 2003 provides that the Coordination Cell Justice shall transfer the data to the requesting authority via an easy-to-use form.

Article 10*bis*, 2° of the Royal Decree of 9 January 2003 provides that the Minister of Justice and the minister competent for electronic communications shall determine the specific format.

In this regard, the "format requirements" set by the European Telecommunications Standards Institute in its TS 101-331 "Lawful Interception (LI); Requirements of Law Enforcement Agencies" may also be considered:[125]

a) The technical handover interfaces shall provide the results of interception for the entire duration of the interception measure.

   NOTE: If a lawful authorization is received during ongoing communication, depending on the intercept implementation, some operational problems might be experienced.

b) These handover interfaces need to be implemented in those telecommunication networks for which the interception capability is required by national laws.

c) The configuration of the handover interface shall ensure that it provides the results of interception.

d) The configuration of the handover interface shall ensure that the quality of service of the telecommunications traffic provided at the handover interface is not inferior to that offered to the target service for each particular call.

---

[125] European Telecommunications Standards Institute, "TS 101-331 Lawful Interception (LI); Requirements of Law Enforcement Agencies," V1.1.1 (2001-08), 4.10.h, available at http://www.etsi.org/deliver/etsi_TS/101300_101399/101331/01.01.01_60/ts_101331v010101p.pdf

e) The configuration of the handover interface shall be such that that the transmission to the LEMF of the result of interception provided at the interface can be implemented with standard, generally available transmission paths, protocols and coding principles.
f) Each interception target shall be uniquely associated with a single instance of the handover interface. This could be achieved by separate channels or the use of identifiers.
g) The correlation between the content of communication and intercept related information shall be unique.
h) LEAs require that the format for transmitting the intercepted telecommunications to the monitoring facility be a generally available format.
i) If network operators/service providers/access providers initiate encoding, compression or encryption of telecommunications traffic, LEAs require the network operators/service providers/access providers to provide intercepted telecommunications en clair.
j) LEAs require network operators/service providers/access providers to be able to transmit the intercepted telecommunications to the LEMF via landline or switched connections.
k) The LEMF/LEA will be informed of: 1) the activation of an intercept measure; 2) the deactivation of the intercept measure; 3) any change of the intercept measure; 4) the temporary unavailability of the intercept measure.

### bb) Transport channels

Article 10*bis*, 1° of the Royal Decree of 9 January 2003 provides that the Coordination Cell Justice shall transfer the data *lege artis* (according to the law of the art), through efficient technical means available on the market.

The European Telecommunications Standards Institute, in its "TS 101-331 Lawful Interception (LI); Requirements of Law Enforcement Agencies," refers to generally available transmission paths:[126]

> The configuration of the handover interface shall be such that that the transmission to the LEMF of the result of interception provided at the interface can be implemented with standard, generally available transmission paths, protocols and coding principles.

### cc) Protocol

Article 10*bis*, 2° of the Royal Decree of 9 January 2003 provides that the Minister of Justice and the minister competent for electronic communications shall determine the transfer modus of data.

---

[126] European Telecommunications Standards Institute, "TS 101-331 Lawful Interception (LI); Requirements of Law Enforcement Agencies," V1.1.1 (2001-08), 4.10.e, available at http://www.etsi.org/deliver/etsi_TS/101300_101399/101331/01.01.01_60/ts_101331v010101p.pdf

In this regard, the reference to "generally available protocols" by the European Telecommunications Standards Institute in its "TS 101-331 "Lawful Interception (LI); Requirements of Law Enforcement Agencies" may be considered:[127]

> The configuration of the handover interface shall be such that that the transmission to the LEMF of the result of interception provided at the interface can be implemented with standard, generally available transmission paths, protocols and coding principles.

### dd) Time limits

Article 126 §2 of the Electronic Communications Act provides that the operators and services shall *immediately* transfer the requested data to the requesting authorities.

Article 5 of the Royal Decree of 9 January 2003 regarding the legal duty to cooperate with judicial requests regarding electronic communications provides that the Coordination Cell Justice shall transfer the data in real time to the National Technical & Tactical Support Unit – Central Technical Interception Facility (NTSU-CTIF) after receipt of the warrant pursuant to Article 90*ter* §1 or §5 CCP. Article 1, 4° of the Royal Decree defines "real time" as the "minimum time necessary for executing a certain performance according to the rules of art, without interruption and with deployment of *adequate means* and personnel" (emphasis added).

Article 6 §1 of the Royal Decree of 9 January 2003 lays down five functional requirements for the data transfer, established in a Council Resolution of 17 January 1995 on the lawful interception of telecommunications.[128] The second functional requirement in Article 6 §1 of the Royal Decree of 9 January 2003 concerns the transfer of interception communications in real time.

In this regard, the reference to "time constraints" by the European Telecommunications Standards Institute in its "TS 101-331 Lawful Interception (LI); Requirements of Law Enforcement Agencies" may also be considered:[129]

> a) A network operator/service provider/access provider shall make the necessary arrangements to fulfil[l] his obligation to enable the interception and delivery of the result of interception from the point in time when the telecommunication installation commences commercial service.

---

[127] European Telecommunications Standards Institute, "TS 101-331 Lawful Interception (LI); Requirements of Law Enforcement Agencies," V1.1.1 (2001-08), 4.10.e, available at http://www.etsi.org/deliver/etsi_TS/101300_101399/101331/01.01.01_60/ts_101331v010101p.pdf

[128] Council of the European Union, Council Resolution of 17 January 1995 on the lawful interception of telecommunications, COM 96/C329/01, OJ C 4 November 1996, pp. 1–6.

[129] European Telecommunications Standards Institute, "TS 101-331 Lawful Interception (LI); Requirements of Law Enforcement Agencies," V1.1.1 (2001-08), 4.5, available at http://www.etsi.org/deliver/etsi_TS/101300_101399/101331/01.01.01_60/ts_101331v010101p.pdf

b) The above requirement applies accordingly to the introduction of modifications to the telecommunication installation or to new operational features for existing telecommunications services to the extent of their impact on existing interception capabilities.

NOTE 1: It is a national implementation (issue for negotiation) whether the operator does this proactively or passively upon request by the LEA.

c) When a lawful authorization is presented a network operator/service provider/access provider shall co-operate immediately.

NOTE 2: If a lawful authorization is received during an ongoing call, depending on the interception implementation, some operational problems might be experienced.

d) After a lawful authorization has been issued, provision of the results of interception of a target identity shall proceed on a real-time or near real-time basis. In the case of near real-time the LEA should be able to force real-time (by means of emptying any buffers involved) if necessary.

### ee) Encryption

The data retention Act of 29 May 2016[130] retained the security measures laid down in Article 125 §5 of the Electronic Communications Act, and complemented them with three additional security measures, including an obligation "to put in place technological protection measures that make the retained data unreadable for any unauthorized individual from the moment of their registration."

### ff) Security measures

The previous version of Article 125 §5 of the Electronic Communications Act laid down the following technical and security measures for providers and operators:

– To guarantee that the retained data are of the same quality and subject to the same security and protection measures as the network data;
– To implement appropriate technical and organizational measures to protect the data against accidental or unlawful destruction, accidental loss or alteration, or unauthorized or unlawful storage, processing, access or disclosure;
– To ensure that data may be accessed by specially authorized personnel only, i.e., the "Coordination Cell Justice," as provided for in Article 2 of the Royal Decree of 9 January 2003 regarding the legal duty to cooperate with regard to judicial requests involving electronic communications;
– To destroy the data at the end of the applicable data retention period.

---

[130] Act of 29 May 2016 on the collection and retention of data in the electronic communications sector, *Belgian Official Journal*, 18 July 2016, entry into force on 28 July 2016.

The Data Retention Act of 29 May 2016[131] retained the security measures laid down in Article 125 §5 of the Electronic Communications Act and complemented them with three additional security measures:

– To store the data on the territory of the EU;
– To put in place technological protection measures that make the retained data unreadable for any unauthorized individuals from the moment of their registration;
– To subject the use of retained data to an efficient traceability process.

Furthermore, the Data Retention Act of 29 May 2016 also requires the appointment of a data protection officer, to ensure that:

– All data processing made by the Coordination Cell Justice complies with the law;
– The operator or operators concerned collect and retain only the data that may be legally retained;
– Only the legally competent authorities have access to the retained data.

The fifth functional requirement in Article 6 §1 of the Royal Decree of 9 January 2003 concerns the secure transfer to prevent data interception by third parties.

Article 10*bis*, 1° of the Royal Decree of 9 January 2003 provides that the Coordination Cell Justice shall transfer the data via a secure transfer.

In this regard, the "information protection requirements" set by the European Telecommunications Standards Institute in its "TS 101-331 Lawful Interception (LI); Requirements of Law Enforcement Agencies" may be considered:[132]

> The technical arrangements required within a telecommunication installation to allow implementation of the interception measures shall be realized with due care exercised in operating telecommunication installations, particularly with respect to:
>
> a) the need to protect information on which and how many target identities are or were subject to interception and the periods during which the interception measures were active;
> b) the restriction to a minimum of staff engaged in implementation and operation of the interception measure;
> c) to ensure the clear delimitation of functions and responsibilities and the maintenance of third-party telecommunications privacy, interception and recording shall be carried out in operating rooms accessible only by authorized personnel;
> d) the result of interception shall be delivered through a handover interface;

---

131 Act of 29 May 2016 on the collection and retention of data in the electronic communications sector, *Belgian Official Journal*, 18 July 2016, entry into force on 28 July 2016.

132 European Telecommunications Standards Institute, "TS 101-331 Lawful Interception (LI); Requirements of Law Enforcement Agencies," V1.1.1 (2001-08), 4.5, available at http://www.etsi.org/deliver/etsi_TS/101300_101399/101331/01.01.01_60/ts_101331v010101p.pdf

e) no access of any form to the handover interface shall be granted to unauthorized persons;
f) network operators, service providers and access providers shall take all necessary measures to protect the handover interface against misuse;
g) the result of interception shall only be transmitted to the LEMF as indicated in the lawful authorization when proof of the authority to receive of the LEMF, and proof of the authority to send of the interface, has been furnished;
h) authentication and proof of authentication shall be implement subject to national laws and regulations;
i) if no dedicated routes to the LEMF are used, such proof shall be furnished for each communication set-up;
j) depending on certain interception cases, LEAs may require confidentiality measures to protect the transmission of the results of such interception. The use of encryption shall be possible;
k) in order to prevent or trace misuse of the technical functions integrated in the telecommunication installation enabling interception, any activation or application of these functions in relation to a given identity shall be fully recorded, including any activation or application caused by faulty or unauthorized input. The records, which are subject to national regulation, shall cover all or some of:
   1) the target identity of the target service or target services concerned;
   2) the beginning and end of the activation or application of the interception measure;
   3) the LEMF to which the result of interception is routed;
   4) an authenticator suitable to identify the operating staff (including date and time of input);
   5) a reference to the lawful authorization.
l) the network operator/service provider/access provider shall ensure that the records are tamper-proof and only accessible to specific nominated staff.

### *e) Checks, filtering, and decryption obligations of communication service providers*

Under Belgian law, there are no checks and filtering obligations that must be performed (automatically or manually) by Internet providers before or during the execution of the interception process. Of note, however, are the checks and filtering standards set by the European Telecommunications Standards Institute in its "TS 101-331 Lawful Interception (LI); Requirements of Law Enforcement Agencies":

4.2. General requirements […]

e) The results of interception relating to a target service shall be provided by the network operator, access provider, service provider in such a way that any telecommunications that do not fall within the scope of the lawful authorization shall be excluded by the network operator, access provider, service provider.

NOTE 5: It is assumed that the intercepting system exercises best effort to exclude non-authorized interception patterns (e.g. transferred communication).[133]

---

[133] European Telecommunications Standards Institute, "TS 101-331 Lawful Interception (LI); Requirements of Law Enforcement Agencies," V1.1.1 (2001-08), 4.2, available at

4.3. Results of interception

The network operator, access provider or service provider shall, in relation to each target service:

a) provide the content of communication;

b) remove any service coding or encryption which has been applied to the content of communication (i.e. en clair) and the intercept related information at the instigation of the network operator or service provider;

NOTE 1: If coding/encryption cannot be removed through means that are available in the network or service for the given communication, the receiving agencies should be provided with keys, etc. to access the information *en clair*, cf. next clause

[…]

e) intercept related information shall contain:

1) the identities that have attempted telecommunications with the target identity, successful or not;

2) identities used by or associated with the target identity;

3) details of services used and their associated parameters;

4) information relating to status;

5) time stamps.[134]

The third functional requirement in Article 6 §1 of the Royal Decree of 9 January 2003 concerns the transfer of encrypted information in a generally accessible format.

The fourth functional requirement in Article 6 §1 of the Royal Decree of 9 January 2003 concerns the transfer of data content in plain language in case the operator of an electronic communications network or the provider of electronic communications introduced encoding, compression, or encryption of the electronic communications traffic. Hence, the transfer takes place without the use of encryption.

## 6. Formal prerequisites of interception orders

### *a) Competent authorities*

Under normal circumstances, the investigating judge authorizes the monitoring measure (Article 90*ter* §1 CCP).

Article 90*ter* §5 CCP provides that, in a *flagrante delicto* case and as long as the *flagrante delicto* situation lasts, the public prosecutor can order the monitoring measure for the criminal offenses referred to in Article 347*bis* CC (on crimes re-

---

http://www.etsi.org/deliver/etsi_TS/101300_101399/101331/01.01.01_60/ts_101331v010101p.pdf

[134] European Telecommunications Standards Institute, "TS 101-331 Lawful Interception (LI); Requirements of Law Enforcement Agencies," V1.1.1 (2001-08), 4.3, available at http://www.etsi.org/deliver/etsi_TS/101300_101399/101331/01.01.01_60/ts_101331v010101p.pdf

garding the taking of hostages) or Article 470 CC (on extortion committed through violence or threats).

Both under normal circumstances, as in the case of *flagrante delicto*, a judicial police officer is designated for the implementation of the measure (Article 90*quater* §1, 5° CCP).

### *b) Formal requirements for applications*

According to Article 61*quinquies* §1 CCP, the suspect and the civil party have the right to request the investigating judge to perform additional investigation methods.

According to Article 61*quinquies* §2 CCP, the suspect and the civil party shall submit their petition for an additional investigation method in writing to the Registry of the Court of First Instance. The petition must be substantiated and give a detailed description of the requested investigation method.

According to Article 61*quinquies* §3 CCP, the judge may reject the request if he considers the measures unnecessary in order to reveal the truth or if, at that moment, he considers the measures prejudicial to the investigation. According to Article 61*quinquies* §4 CCP, rejection by the investigating judge is subject to appeal before the Indictment Chamber (see I.A.4.b.), in which case the investigating judge shall hear the Prosecutor General, the suspect, and his or her attorney (Article 61*quater* §5 CCP).

### *c) Formal requirements for orders*

Article 90*quater* CCP reads as follows:

> §1 The investigating judge authorizes each monitoring measure under Article 90ter by a reasoned decision, and communicates the warrant to the public prosecutor.
>
> The warrant shall be dated and mentions:
>
> 1) the indications and concrete facts specific to the case, which justify the measure under Article 90ter;
> 2) the reasons why the measure is necessary to reveal the truth;
> 3) the person, the (tele-)communications method or the place that is the subject of the monitoring measure;
> 4) the period during which the monitoring measure can be carried out, which should not be longer than one month counting from the decision by which the measure is ordered;
> 5) the name and the capacity of the judicial police officer designated for the implementation of the measure.

The Act of 5 February 2016 deleted the prescription of this provision on penalty of nullity.[135]

## 7. Substantive prerequisites of interception orders

### *a) Degree of suspicion*

According to Article 90*ter* §1 CCP, the investigating judge may wiretap, take cognizance of, and record private (tele-)communications if there are "serious indications" of a criminal offense.

### *b) Predicate offences*

In the wake of the terrorist attacks against the French satirical magazine Charlie Hebdo on 7 January 2015, the Belgian legislator extended the list of terrorism crimes that can justify an interception measure. Thereto, the Law of 20 July 2015[136] amended Article 90*ter* §2, 1°*ter* CCP to include *all*, and not just three, terrorism crimes, provided in Book II, title I*ter* of the Criminal Code:[137]

- Article 137 – on the execution of terrorism crimes;
- Article 138 – on penalties for terrorism crimes;
- Article 139 – on the definition of a terrorist group;
- Article 140 – on participating in or financing the activities of a terrorist group, supplying information or material resources to a terrorist group, and leading a terrorist group;
- Article 140*bis* – on publicly spreading a message in order to incite to terrorism crimes;
- Article 140*ter* – on recruiting persons for the execution of terrorism crimes;
- Article 140*quater* – on giving instructions or education to fabricate explosives, firearms or other weapons or harmful or dangerous substances;
- Article 140*quinquies* – on taking instructions or education to fabricate explosives, firearms or other weapons or harmful or dangerous substances;
- Article 140*sexies* – on leaving or entering the territory to commit terrorism crimes in Belgium or abroad;

---

[135] Act of 5 February 2016 regarding the modification of criminal law and criminal procedure and regarding diverse provisions on criminal policy, *Belgian Official Journal*, 19 February 2016, entry into force on 29 February 2016.

[136] Act of 20 July 2015 to strengthen the fight against terrorism, *Belgian Official Journal*, 5 August 2015, entry into force on 15 August 2015.

[137] The previous version of Article 90*ter* §2, 1°*ter* CCP referred to only three articles in Book II, title I*ter* of the Criminal Code (Article 137, Article 140, and Article 141).

– Article 141 – on supplying material resources, including financial support, to commit one of the terrorist crimes provided in Article 137;
– Article 141*bis* – on the non-application of this title to the acts of armed forces during armed conflict or in the fulfillment of their official duties insofar governed by other rules of international law;
– Article 141*ter* – on the non-derogation from fundamental rights protection.

One month after the terrorist attacks in Brussels on 22 March 2016, the Belgian legislator once more extended the list of terrorism crimes that can justify an interception measure. The Act of 27 April 2016[138] retained the reference in Article 90*ter* §2, 10° CCP to the six articles under Book II, title IX, chapter I, section II*bis* of the Criminal Code; and, in addition, it included reference in the same Article 90*ter* §2, 10° CCP to *all*, and not just one of the, nuclear crimes in Book II, title IX, chapter I*bis* of the Criminal Code.[139]

– Article 488*bis* – on the unlawful delivery, possession, use, modification, cession, leaving behind, transport or distribution of, or committing an act against, nuclear materials;
– Article 488*ter* – on the unlawful preservation, fabrication, use of, or committing an act against, radioactive materials other than nuclear materials;
– Article 488*quater* – to demand – via threats that seem credible in the circumstances, or on the basis of violence – the transfer of nuclear materials, nuclear instruments or nuclear installations;
– Article 488*quinquies* – on unlawful intrusion (or attempt thereto) into a nuclear installation.

The same Act of 27 April 2016 also complements Article 90*ter* §2, 16° CCP with the following list of Belgian laws:
– Article 16 of the Decree of the Flemish Parliament of 15 June 2012 on the import, export, transit and transfer of defense-related products, other material for military use, law enforcement equipment, civilian firearms, parts and ammunition;
– Article 20 of the Decree of the Walloon Region of 21 June 2012 on the import, export, transit and transfer of civil weapons and defense-related products;
– Article 42 of the Ordonnance of the Brussels Capital Region of 20 June 2013 on the import, export, transit and transfer of defense-related products, other material

---

[138] Act of 27 April 2016 on additional measures to fight terrorism, *Belgian Official Journal*, 9 May 2016, entry into force on 19 May 2016.

[139] The previous version of Article 90*ter* §2, 10° CCP also referred to the six articles under Book II, title IX, chapter I, section II*bis* of the Criminal Code (Articles 477, 477*bis*, 477*ter*, 477*quater*, 477*quinquies*, 477*sexies* – on the theft and extortion of nuclear materials). But it referred to only article under Book II, title IX, chapter I*bis* of the Criminal Code (Article 488*bis*).

for military use, law enforcement equipment, civilian firearms, parts, accessories and its ammunition;

– Articles 8 to 11, 14, 16, 19, 1°, 2°, 3°, 5° and 6°, 20, 22, 27 and 33 of the Act of 8 June 2006 on the regulation of economic and individual activities with weapons, also called the "Arms Act";
– The Act of 28 May 1956 on explosives and the deflagration substances and mixtures and thereby loaded vehicles;
– Articles 21 to 26 of the Cooperation Agreement between the Federal State, the Flemish Region, the Walloon Region and the Brussels Capital Region concerning the implementation of the Convention on the prohibition of the development, production, stockpiling and use of chemical weapons and on their destruction, Paris 13 January 1993.

The current version of Article 90*ter* §2 CCP provides the following list of offences that can justify a monitoring measure:

– 1° Articles 101 to 110 of the Criminal Code [on the attack and conspiracy against the King, the royal family and the form of government];
– 1°*bis* Articles 136*bis* [on genocide], 136*ter* [on crimes against humanity], 136*quater* [on war crimes], 136*sexies* [on producing, keeping or transporting a tool, a device or any object, and constructing a building or changing a building to commit one of the crimes provided in Article 136*bis*, 136*ter*, and 136*quater*] and 136*septies* of the same Code [on ordering, proposing, accepting, inciting, attempting to commit one of the crimes provided in Article 136*bis*, 136*ter*, and 136*quater*, as well as participating in, and the failure to prevent, the commission of these crimes], and Article 41 of the Law of 29 March 2004 regarding the cooperation with the International Criminal Court and the international criminal tribunals [crimes against the administration of justice of the International Criminal Court];
– 1°*ter* Book II, title I*ter* of the same Code [on terrorism crimes]: Article 137 [on the execution of terrorism crimes]; Article 138 [on penalties for terrorism crimes]; Article 139 [on the definition of a terrorist group]; Article 140 [on participating in or financing the activities of a terrorist group, supplying information or material resources to a terrorist group, and leading a terrorist group]; Article 140*bis* [on publicly spreading a message in order to incite to terrorism crimes]; Article 140*ter* [on recruiting persons for the execution of terrorism crimes]; Article 140*quater* [on giving instructions or education to fabricate explosives, firearms or other weapons or harmful or dangerous substances]; Article 140*quinquies* [on taking instructions or education to fabricate explosives, firearms or other weapons or harmful or dangerous substances]; Article 140*sexies* [on leaving or entering the territory to commit terrorism crimes in Belgium or abroad]; Article 141 [on supplying material resources, including financial support, to commit one of the terrorist crimes provided in Article 137];

Article 141*bis* [on the non-application of this title to the acts of armed forces during armed conflict or in the fulfillment of their official duties insofar governed by other rules of international law]; Article 141*ter* [on the non-derogation from fundamental rights protection];

- 1°*quater* Article 210*bis* of the same Code [forgery through entering, changing or deleting computer data or through altering their potential use, if this causes a change in the legal scope of such data];
- 1°*quinquies* Articles 246, 247, 248, 249, 250 and 251 of the same Code [on the bribery of persons exercising a public function];
- 1°*sexies* Article 259*bis* of the same Code [on wiretapping, taking cognizance and recording of private (tele-)communications by public officials];
- 1°*septies* Article 314*bis* of the same Code [on the prohibition, applicable to everyone, of taking knowledge of the content, during the transfer, of private (tele-) communications one does not participate in];
- 1°*octies* Articles 324*bis* and 324*ter* of the same Code [on criminal organisations].
- 2° Articles 327, 328, 329 or 330 of the same Code [on threating to attack persons or property and giving false information on serious attacks], to the extent that a complaint has been filed;
- 3° Article 331*bis* of the same Code [on the harmful use of radioactive materials or instruments];
- 4° Article 347*bis* of the same Code [on crimes regarding the taking of hostages];
- 4°*bis* […]
- 5° Articles 379 and 380 of the same Code [on the decay of youth and prostitution].
- 6° Article 393 of the same Code [on manslaughter];
- 7° Articles 394 [on murder] or 397 [on intoxication] of the same Code;
- 7°*bis* Articles 428 and 429 of the same Code [on kidnapping of minors];
- 7°*ter* Articles 433*sexies*, 433*septies* and 433*octies* of the same Code [on human trafficking];
- 8° Articles 468, 470, 471 or 472 of the same Code [on theft committed through violence or threats, and extortion];
- 9° Article 475 of the same Code [on manslaughter to facilitate or ensure the impunity of theft or extortion];
- 10° Book II, title IX, chapter I, section II*bis*, and chapter I*bis* of the Criminal Code: Articles 477, 477*bis*, 477*ter*, 477*quater*, 477*quinquies*, 477*sexies* [on the theft and extortion of nuclear materials]; Article 488*bis* [on the unlawful delivery, possession, use, modification, cession, leaving behind, transport or distribution of nuclear materials] of the same Code; Article 488*ter* [on the unlawful

preservation, fabrication, use of, or committing an act against, radioactive materials other than nuclear materials]; Article 488*quater* [to demand – via threats that seem credible in the circumstances, or on the basis of violence – the transfer of nuclear materials, nuclear instruments or nuclear installations]; Article 488*quinquies* [on unlawful intrusion (or attempt thereto) into a nuclear installation];

- 10°*bis* Articles 504*bis* and 504*ter* of the same Code [on private commercial bribery];
- 10°*ter* Article 504*quater* of the same Code [on computer fraud];
- 11° Article 505 (first paragraph, 2°, 3° and 4°) of the same Code [on receiving of, and other transactions relating to, objects resulting from a criminal offense];
- 12° Articles 510, 511, first paragraph or 516 of the same Code [on arson];
- 13° Article 520 of the same Code [on the destruction of constructions by causing an explosion], if the circumstances referred to in Articles 510 or 511, first paragraph, of the same Code are united;
- 13°*bis* Articles 550*bis* [on hacking] and 550*ter* [on data and system interference] of the same Code;
- 14° Article 2*bis*, §3, b [on offences regarding narcotics or stupefying substances, other psychotropic substances that may cause dependency, or cultivating of plants to extract these substances, that consist in the participation in the activities of an association] or §4, b [on the same offences but committed in the capacity of a leading person] of the Law of 24 February 1921 concerning the trafficking of poisonous, narcotic, stupefying, psychotropic, disinfectant and antiseptic substances;
- 15° Article 145 §3 [on the fraudulent making of electronic communications through a network of electronic communications, in order to provide oneself or another an unlawful benefit] and §3*bis* [on the use of an electronic communications network or provider, or of other electronic communication methods, to cause nuisance to his correspondent or to cause harm, or setting up a device intended to commit the previous offences] of the Law of 13 June 2005 on electronic communications;
- 16° Article 10 of the Law of 5 August 1991 on the import, export and transit of arms, ammunition and materials specifically intended for military use and the associated technology [on illegal trade in weapons, ammunition and materials specifically intended for military use and the associated technology];
- 16°*bis* Article 16 of the Decree of the Flemish Parliament of 15 June 2012 on the import, export, transit and transfer of defense-related products, other material for military use, law enforcement equipment, civilian firearms, parts and ammunition;

- 16°*ter* Article 20 of the Decree of the Walloon Region of 21 June 2012 on the import, export, transit and transfer of civil weapons and defense-related products;
- 16°*quater* Article 42 of the Ordonnance of the Brussels Capital Region of 20 June 2013 on the import, export, transit and transfer of defense-related products, other material for military use, law enforcement equipment, civilian firearms, parts, accessories and its ammunition;
- 16°*quinquies* Articles 8 to 11, 14, 16, 19, 1°, 2°, 3°, 5° and 6°, 20, 22, 27 and 33 of the Act of 8 June 2006 on the regulation of economic and individual activities with weapons, also called the "Arms Act";
- 16°*sexies* of the Act of 28 May 1956 on explosives and the deflagration substances and mixtures and thereby loaded vehicles;
- 16°*septies* Articles 21 to 26 of the Cooperation Agreement between the Federal State, the Flemish Region, the Walloon Region and the Brussels Capital Region concerning the implementation of the Convention on the prohibition of the development, production, stockpiling and use of chemical weapons and on their destruction, Paris 13 January 1993;
- 17° Articles 77*ter*, 77*quater* and 77*quinquies* of the Law of 15 December 1980 on access to the territory, residence, establishment and removal of foreigners [on human trafficking];
- 18° Article 10, §1, 2° of the Law of 15 July 1985 regarding the use in animals of substances with hormonal, anti-hormonal, beta-adrenergic or production stimulating effects [on the offences relating to the administration of substances, and the trade in animals to which substances were unlawfully administered];
- 19° Article 1 of the Royal Decree of 12 April 1974 with respect to some actions relating to materials with a hormonal, anti-hormonal, anabolic, beta-adrenergic, anti-infectious, anti-parasitic and anti-inflammatory effect, which concerns criminal offenses for which criminal sanctions are provided by the Law of 24 February 1921 concerning the trafficking of poisonous, narcotic, stupefying, psychotropic, disinfectant and antiseptic substances [on the licence for the actions relating to these materials].

Article 90*ter* §4 CCP provides that:

> [a] criminal offense, referred to in Articles 322 or 323 of the Criminal Code [on associations with a view to commit an attack on persons or property] may also justify a monitoring measure, to the extent that the association is formed with the aim to commit an attack against the persons or properties referred to in §2, or to commit the criminal offence referred to in article 467, first paragraph, of the Criminal Code [on theft though burglary, climbing through, false keys, or by a public official through his ministry].

The potential or the likely sentencing range for the offenses listed in Article 90*ter* §§2 and 4 does not serve as additional mitigating criteria.

### *c) Persons and connections under surveillance*

Article 90*ter* §1, 3° CCP provides that the monitoring measure can be ordered in respect of:

1) the (tele-)communications methods that are regularly used by a suspected person

2) or in respect of places where he is suspected to stay

3) or in respect of persons who are suspected, on the basis of specific facts, to have regular communications with a suspected person.

The parliamentary preparatory works specify that proactive monitoring is prohibited (cf. supra I.A.2.b.), for instance in relation to a reputed criminal: the application of Article 90*ter* CCP depends on the existence of a suspect.[140]

### *d) Principle of subsidiarity*

According to Article 90*ter* §1 CCP, the investigating judge may only carry out a wiretapping measure if the other investigation methods are not sufficient to reveal the truth. The parliamentary preparatory works note, however, that there is no need for a prior unsuccessful application of the other investigation methods by the investigating judge: it suffices that the investigating judge considers the other measures unlikely to be successful.[141]

### *e) Proportionality of interception in individual cases*

There is an obligation for the investigating judge to verify that the interception is proportionate to the seriousness of the offense in the individual case. According to Article 90*ter* §1 CCP, the investigating judge may wiretap, take cognizance of, and record private (tele-)communications only in *exceptional cases*.

Van den Wyngaert relates the proportionality principle to the list of offenses provided in Article 90*ter* §2 CCP, which can justify a monitoring measure (see section III.B.7.b.).[142] Hence, monitoring measures that are ordered for other offenses than the ones listed in Article 90*ter* §2 violate the principle of proportionality.

---

[140] Parliamentary preparatory works, regarding the legislative proposal protecting privacy against the interception of communication and telecommunication, Belgian Senate, 1992-1993, 1 September 1993, no. 843-1, p. 15, available at http://www.senate.be/lexdocs/S0539/S05390297.pdf

[141] Parliamentary preparatory works, regarding the legislative proposal protecting privacy against the interception of communication and telecommunication, Belgian Senate, 1992-1993, 1 September 1993, no. 843-1, p. 14, available at http://www.senate.be/lexdocs/S0539/S05390297.pdf

[142] Chris Van den Wyngaert, *Strafrecht, Strafprocesrecht & Internationaal Strafrecht in hoofdlijnen* (An Outline of Criminal Law, Criminal Procedural Law & International Criminal Law), Antwerp-Apeldoorn, Maklu, 2006, p. 983.

Freyne distinguishes three subcriteria of the proportionality principle: the seriousness of the offense, the finality/purpose of the monitoring measure (the protection of public order or public security), and the breach of the legal order.[143] Hence, there is no specific requirement regarding the likelihood that the anticipated evidence will actually be obtained by means of the requested monitoring measure.

#### *f) Consent by a communication participant to the measure*

As said earlier (section III.B.6.b.), according to Article 61*quinquies* §3 CCP, the judge may reject the request by the suspect or a civil party if he considers the measures unnecessary in order to reveal the truth or if, at that moment, he considers the measures prejudicial to the investigation. Hence, the consent by a communication participant to the measure is not a decisive prerequisite for the interception order.

### 8. Validity of interception order

#### *a) Maximum length of interception order*

Article 90*quater* §1, 4° CCP provides that, on penalty of nullity, the warrant shall be dated and mention "the period during which the monitoring measure can be carried out, which should not be longer than one month counting from the decision by which the measure is ordered."

#### *b) Prolongation of authorization*

In both normal circumstances and cases of emergency, Article 90*quinquies* CCP allows prolongation and renewal of the monitoring warrant:

> The investigating judge may extend the effect of its warrant one or more times by a period not longer than one month, with a maximum of six months, without prejudice to its decision to end the measure as soon as the circumstances that justified the measure have disappeared. The provisions in article 90quater, §1, are applicable to the extension referred to in the preceding paragraph. The warrant shall also mention the precise circumstances, which justify the extension of the measure.
>
> If new and serious circumstances necessitate the measures referred to in Article 90*ter*, then the investigating judge may order a new measure, in compliance with the formalities set out in Articles 90*ter* and 90*quater*. In that case, the warrant must state the precise new and serious circumstances that necessitate and justify a new measure.

Hence, the prolongation or renewal of the monitoring measure follows the same procedure as the initial application for a monitoring measure.

---

[143] Thierry Freyne, "De bewaking van privécommunicatie en -telecommunicatie in strafonderzoeken: een stand van zaken" (The monitoring of private communications and telecommunications in criminal proceedings: a state of affairs), *Tijdschrift voor Strafrecht,* 2008, vol. 3, p. 172, no. 17.

*c) Revocation of authorization*

In both normal circumstances and cases of emergency, Article 90*quinquies* §1 CCP allows revocation of the monitoring warrant:

> The investigating judge may extend the effect of its warrant one or more times by a period not longer than one month, with a maximum of six months, without prejudice to its decision to end the measure as soon as the circumstances that justified the measure have disappeared.

Freyne holds that the investigating judge has a duty to revoke the authorization during the monitoring measure in case it becomes apparent that other investigation methods are sufficient to reveal the truth (principle of subsidiarity, see section III.B.7.d. above).[144]

## 9. Duties to record, report, and destroy

*a) Duty to record and report*

As said above, a set of articles regulates the general exchange of data between the police service and law enforcement authorities (section I.A.4.a.).

Article 15, 1° of the Act of 5 August 1992 on the Police Function reads as follows:

> In the performance of their judicial police functions, the police have the task: 1° to detect the crimes, misdemeanours and contraventions, to gather evidence thereof, to notify the competent authorities thereof, to apprehend and arrest the perpetrators, to bring them at the disposal of the competent authorities, in the manner and forms provided by law;

Article 53 CCP adds that the judicial police officers shall immediately send the reports (of an offense), official records, and any other acts drafted under their competence to the public prosecutor. This provision is echoed by Article 40 of the Act of 5 August 1992 on the Police Function, which provides that police officers shall send the official records on complaints, reports of offenses, the intelligence and any detections to the competent judicial authorities.

Article 54 CCP adds that the judicial police officers shall also immediately send any reports of crimes and misdemeanours they are not competent to deal with to the public prosecutor.

Article 5/3 of the Act of 5 August 1992 on the Police Function adds that, in order to perform judicial police functions, the police shall maintain regular *service relations* with the local public prosecutors, the federal public prosecutor, and the Prosecutors General.

---

[144] Thierry Freyne, "De bewaking van privécommunicatie en -telecommunicatie in strafonderzoeken: een stand van zaken" (The monitoring of private communications and telecommunications in criminal proceedings: a state of affairs), *Tijdschrift voor Strafrecht*, 2008, vol. 3, p. 173, no. 18.

More specifically regarding the monitoring measure, first, Article 90*quater* §3, 2° CCP provides that "[t]he designated judicial police officers report at least every five days in writing to the investigating judge on the implementation of the warrant."

Second, Article 90*sexies* CCP reads as follows:

> §1 The designated judicial police officers shall provide the investigating judge with:
>
> 1° the file with the recordings made as a result of the measures taken in application of Articles 90ter, 90quater and 90quinquies;
>
> 2° the transcription of the parts[145] of the (tele-)communications that the designated judicial police officer deems relevant for the investigation, and its possible translation;
>
> 3° what the irrelevantly deemed (tele-)communications concerns, the cited topics and the identification of the (tele-)communications means to which or from which was called.

According to Article 90*septies* §1 CCP, the data mentioned in Article 90*sexies* CCP do not necessarily need to be recorded in an official record (see the following section).

### *b) Duty to destroy*

With regard to the monitoring measure on the part of the Belgian investigating judge, Article 90*septies* §1 CCP reads as follows:

> Every record in the context of the implementation of the measures referred to in the preceding paragraph by the designated persons, which is not recorded in an official record, is destroyed, except for the transcription of the parts of the relevantly deemed (tele-) communications of the record, any translation thereof, and what the irrelevantly deemed (tele-)communications concerns, the cited topics and the identification of the telecommunications means to which or from which was called. The judicial police offer designated for the implementation of the measure undertakes the destruction and states this in an official record.

Hence, both relevantly deemed parts of (tele-)communications and irrelevantly deemed (tele-)communications are not destroyed.

With regard to the monitoring measure by foreign authorities, Article 90*ter* §6, 1° CCP provides that:

> [a] competent foreign authority may, within the framework of a criminal investigation, temporarily wiretap, take cognizance of, and record private telecommunications during transmission, if the person to whom this measure applies is located on the Belgian territory,

---

[145] The Act of 5 February 2016 amended Article 90*sexies* CCP by deeming it sufficient that the designated judicial police officers shall provide the investigating judge with only *parts* of (tele-)communications that the designated judicial police officer deems relevant for the investigation. Act of 5 February 2016 regarding the modification of criminal law and criminal procedure and regarding diverse provisions on criminal policy, *Belgian Official Journal*, 19 February 2016, entry into force on 29 February 2016.

under certain conditions provided in its paragraph 2 including the notification of the measure to a Belgian judicial authority.

Article 90*ter* §7 *in fine* CCP provides that:

> [i]f the investigating judge does not allow the measure referred to in §6, it shall also notify the foreign government that the gathered data must be destroyed and cannot be used.

## 10. Notification duties and remedies

### *a) Duty to notify persons affected by the measure*

Article 90*sexies in fine* CCP reads as follows:

> The warrants of the investigating judge, the reports of the judicial police officers referred to in Article 90quater, §3, and the official records relating to the implementation of the measure, are included in the file at the latest by the end of the measure.

Van den Wyngaert specifies that these documents are included in the file at the latest 15 days after the end of the measure, which is also the deadline for notifying the persons subject to a monitoring measure (see below in this section).[146] The suspect has access to the judicial file (Article 61*ter* CCP).

As third parties do not have access to the judicial file, Article 90*novies* CCP lays down a notification duty towards *any* person subject to a monitoring measure:

> Not later than fifteen days after the decision on the administration of justice becomes final, or after the deposit of summons referred to in Article 524b, §6 at the Registry of the tribunal or the court, the Registrar shall, at the request of the public prosecutor or where appropriate the Prosecutor General, inform in writing any person against whom a measure was taken under Article 90ter, of *the nature of the measure and the days on which the measure was executed*. (italics added)

Arnou notes that the duty of notification of the nature of measure and the days on which it was executed is not prescribed under sanction of nullity (see below, section IV.2.). Nor do the parliamentary preparatory works provide any clarity in this regard. In any case, no exclusion will follow on the basis of an alleged violation of the rights of defense because, as said, the suspect has access to the judicial file on the basis of Article 61*ter* CCP. Arnou says further that, at most, a disciplinary sanction or civil sanction will be allowed.[147]

Unfortunately, the Board of Public Prosecutors could not positively respond to our request of 2 April 2015 to obtain data on infringements of the laws on intercep-

---

[146] Chris Van den Wyngaert, *Strafrecht, Strafprocesrecht en internationaal strafrecht in hoofdlijnen* (An Outline of Criminal Law, Criminal Procedural Law & International Criminal Law), Antwerp-Apeldoorn, Maklu, 2009, p. 1058.

[147] Luc Arnou, "Afluisteren tijdens het gerechtelijk onderzoek" (Wiretapping during the investigation); in Commentaar Strafrecht en strafvordering (Commentary criminal law and criminal procedural law), Gent, Kluwer, 2008, vol. 59, pp. 80–81, no. 83.

tion of telecommunications. Hence, it not possible to report on the notification practices.

*b) Remedies*

Article 90*ter* and following of the CCP are silent regarding the remedies available to the suspect during the interception. As said in the previous section, Article 90*novies* CCP lays down a notification duty towards any person subject to a monitoring measure fifteen days after the end of the measure.

However, the general rules of criminal procedure apply as regards the remedies that are available to a person who becomes aware that he/she was subject to an illegally performed monitoring measure. As already said (see section II.A.3.), the Courts in Chambers (court of instruction in first instance) and the Indictment Chamber (court of instruction in appeal) evaluate the legality of the evidence collection during the investigation phase (Article 131 CCP, Article 135 §2 CCP, and Article 235*bis* §6 CCP). Both the Courts in Chambers[148] and the Indictment Chamber determine the grounds for finding a nullity on the basis of the so-called Antigoon criteria (see below, section IV.2.). The lack of rationale may give rise to an appeal against the decision of the Courts in Chambers before the Chamber of Indictment (Article 135 §2 CCP) and against the decision of the latter before the Supreme Court (Article 235*bis* §6 CCP *versus* Article 416 CCP). The proceedings before the Courts in Chambers and the Indictment Chamber are public and adversarial (Article 127 §4 CCP, respectively Article 135 §3 CCP).

If the Courts in Chambers finds no illegality, and the parties do not appeal this decision before the Court of Indictment, then they can raise this point again before the trial judge. If the parties do appeal this decision before the Indictment Chamber decides, then they cannot raise this point again before the trial judge except when the alleged nullity concerns the weighing of evidence, which is an exclusive task of the trial judge (Article 235*bis* §5 CCP).

It is of note that illegally obtained files are not destroyed but instead removed from the judicial file and kept at the Registry of the Court of First Instance (Article 235*bis* §6 CCP). The Indictment Chamber decides who can have access to the removed files in light of the right of defense. In this regard, the Supreme Court also

---

[148] Unlike the Indictment Chamber (Article 235*bis* CCP), the Courts in Chambers can only evaluate evidence during the investigation phase and not during the preliminary investigation phase: more particularly, the Courts in Chambers evaluates the evidence during the formal closure of the investigation phase during the so-called settlement of proceedings (*Regeling van de rechtspleging* in Dutch; *règlement de la procédure* in French). See Brigitte Pesquié (revised by Yves Cartuyvels), "The Belgian system", in Mireille Delmas-Marty and John R. Spencer, *European Criminal Procedures*, Cambridge Studies in International and Comparative Law, Cambridge University Press, 2002, (81) 109.

held that the trial judge may allow parties access to the removed documents that are essential for the right of defense.[149]

*c) Criminal consequences of unlawful interception measures*

The Board of Public Prosecutors could not positively respond to our request of 2 April 2015 to obtain data on the infringements of the laws on interception of telecommunications. Hence, it is not possible to list specific sanctions imposed on officials for wrongfully conducting a monitoring measure, nor to provide the frequency with which such cases occurs or sanctions are imposed.

As noted earlier (section III.B.10.a.), at most, a disciplinary sanction or civil sanction would be allowed for violations of the notification duty.[150]

We also recall that the monitoring measure in Article 90*ter* CCP provides an exception to the general prohibition of the interception of (tele-)communications (Article 314*bis* CC and Article 259*bis* CC, see section II.A.4.a.).

## 11. Confidentiality requirements

*a) Obligations of telecommunication service providers to maintain secrecy*

As said above (section III.B.5.b.), Article 90*quater* §2 and §4 CCP lays down the cooperation duties for individuals and the private sector. Both provisions lay down a specific obligation for Internet providers and individuals to keep their support measures confidential.

Article 90*quater* §2, 1° CCP reads as follows:

> §2. If the measure involves an operation on a communications network, then is the operator of this network or the provider of the telecommunications service obliged to provide technical cooperation, if the investigating judge requests so directly or via a by the King designated police service.[151]

Article 90*quater* §4, 1-2° CCP reads as follows:

> §4 The investigating judge can order, directly or via a by the King designated police service, persons of whom he thinks that they have special knowledge of the telecommunications service subject to the monitoring measure, or of services used to protect or en-

---

[149] Supreme Court, 18 February 2003, P020913N.

[150] Luc Arnou, "Afluisteren tijdens het gerechtelijk onderzoek" (Wiretapping during the investigation); in Commentaar Strafrecht en strafvordering (Commentary criminal law and criminal procedural law), Gent, Kluwer, 2008, vol. 59, pp. 80–81, no. 83.

[151] The Act of 5 February 2016 amended Article 90quater §2, 1° CCP and Article 90*quater* §4, 1-2° CCP, and added the possibility for the investigating judge to request technical cooperation via a by the King appointed police service. Act of 5 February 2016 regarding the modification of criminal law and criminal procedure and regarding diverse provisions on criminal policy, *Belgian Official Journal*, 19 February 2016, entry into force on 29 February 2016.

> crypt data that are stored, processed, encrypted or transferred via a computer system, to provide information on the operation of the system and on the way to get access to the content of the telecommunication, that is or has been transferred, in an understandable format.
>
> He can order persons to make the content of telecommunications accessible in the format requested by him. These persons are obliged to comply with the order, to the extent of their capabilities.

*b) Sanctions against telecommunication service providers and their employees*

Both articles discussed in the previous section lay down specific sanctions for infringements of their obligations.

Article 90*quater* §2, 2° and 3° CCP reads as follows:

> §2 […]
>
> Any person, who by virtue of his office is informed of the measure or cooperates thereto, is bound by secrecy. Any violation of secrecy shall be punished in accordance with Article 458 of the Penal Code.
>
> Any person who refuses technical cooperation to the requests referred to in this article, of which the modalities are determined by the King, is punished with a fine of twenty six francs to ten thousand francs on the proposal of the Minister of Justice and the Minister competent for Telecommunications.

Article 90*quater* §4, 3-5° CCP reads as follows:

> §4 […]
>
> He who refuses to provide the cooperation ordered in accordance with the preceding paragraphs shall be punished with imprisonment of six months to one year and a fine of twenty six francs to twenty thousand francs or one of these penalties.
>
> Any person who by virtue of his ministry receives notification of the measure or who is called to granting technical cooperation is bound to the secrecy of the judicial investigation.
>
> Any person, who by virtue of his office is informed of the measure or is called to grant technical cooperation, is bound to secrecy. Any violation of secrecy shall be punished in accordance with Article 458 of the Criminal Code.

A circular of the Board of Prosecutors General of 17 December 2009 explains the criminal policy regarding violations of the cooperation duties under Article 46*bis* §2 CCP (collection of identification data of electronic communications), Article 88*bis* §2 CCP (tracing of traffic data, and localization of electronic communications), and Article 90*quater* §2 CCP.[152] An investigation follows from manifest

---

[152] Board of Prosecutors General, "Telecommunicatierichtlijn inzake het opsporings- en vervolgingsbeleid betreffende inbreuken op de medewerkingsverplichtingen vervat in de artikelen 46bis § 2, 88bis § 2 en 90quater § 2 van het wetboek van strafvordering" (Telecommunications Circular regarding the investigation and prosecution of violations of the cooperation duties under Articles 46*bis* §2, 88*bis* § 2 and 90*quater* § 2 CCP), COL 14/2009, 17 December 2009, available (in Dutch and French) at http://www.om-mp.be/omzendbrief/4420834/col_14-2009_dd__17_12_2009.html

refusals to cooperate. In other cases, an adequate reaction will depend on the seriousness of the infringement or the specific circumstances.

No specific sanctions are foreseen for violations of the earlier discussed security requirements for data transfers by communication service providers (section III.B.5.d.).

## C. Collection and Use of Traffic Data and Subscriber Data

### 1. Collection of traffic data and subscriber data

#### *a) Collection of traffic data*

##### aa) Relevant information

The Data Retention Act of 29 May 2016 added eight amendments to Article 88*bis* CCP:

1) Replacement of the term "telecommunications" with the term "electronic communications";
2) An additional application requirement for the measure: in addition to the already existing requirement that the investigating judge find circumstances that necessitate the application of the measure, from now on serious indications also need to exist that the criminal facts can result in the imposition of a correctional penalty of one-year imprisonment or a higher penalty;
3) The investigating judge can now also request cooperation via a police service designated by the King;
4) Inclusion of the principles of proportionality and subsidiarity;
5) The possibility to order the measure orally in case of emergency, in which case the measure must be confirmed as soon as possible in the form set out in the third and fourth paragraph of Article 88*bis* CCP.
6) If the measure applies to the traffic or localization data retained under Article 126 of the Act of 13 June 2005 on electronic communications, then the warrant also needs to mention the past period to which the warrant refers.
7) A new paragraph 2 on the application of the measure to the traffic or localization data retained under Article 126 of the Act of 13 June 2005 on electronic communications. The following rules apply:

   For a criminal offense referred to in Book II, Title I*ter* of the Criminal Code [terrorism crimes], the investigating judge in his warrant may request the data for a period of twelve months prior to his warrant;

   For another criminal offense referred to in Article 90ter, §§2 to 4, which is not referred to in the first indent, or a criminal offense which was committed within the framework of a criminal organization as defined in Article 324bis of the Criminal Code, or a criminal offense that may result in five years imprisonment or a more severe penalty, the

investigating judge in his warrant may request the data for a period of nine months prior to the warrant;

For other offenses, the investigating judge may only request the data for a period of six months prior to the warrant.

8) A new paragraph 3 on professional secrecy, which reflects Article 90*octies* (wiretapping). New paragraph 3 reads as follows:

The measure may only cover the electronic communications of a lawyer or a doctor, who themselves are suspected of having committed or participated in one of the criminal offenses referred to in the first paragraph, or if specific facts suggest that third parties suspected of having committed a criminal offense referred to in the first paragraph, use their electronic communications.

The measure may not be implemented if, depending on the case, the president of the Bar or the representative of the provincial council of the order of physicians have not been informed of it. They will be informed by the investigating judge of what according to him shall be covered by professional secrecy. These data shall not be recorded in the official record.

Article 88*bis* CCP refers to the tracing of traffic data, and localization of electronic communications. Article 88*bis* §1 CCP describes the relevant information:

- tracing traffic data of electronic communications means from which or to which electronic communications are or were made.
- locating the origin or the destination of electronic communications

Article 88*bis* §1 CCP lays down the prerequisites for the tracing of traffic data, and localization of electronic communications:[153]

§1. In case of serious indications that the criminal facts can result in the imposition of a correctional penalty of one year imprisonment or of a higher penalty, and the investigating judge finds circumstances that necessitate the tracing of electronic communications or the localisation of the origin or the destination of electronic communications in order to find the truth, then he can, directly or via a police service designated by the King request the cooperation of an operator of an electronic communications network or the provider of an electronic communications service, to proceed or initiate to proceed to

- tracing traffic data of electronic communications means from which or to which electronic communications are or were made.
- locating the origin or the destination of electronic communications.

In the cases provided for in the first paragraph, the day, time, duration, and, if necessary, the place of the call for each telecommunications method of which the call data are detected or of which the destination of the telecommunications is localized, shall be determined and included in an official record.

In a reasoned warrant, the investigating judge states the factual circumstances of the case that justify the measure, and the proportionality in relation to the privacy and the subsidiarity in relation to any other investigatory act.

He also mentions the duration of the measure, which shall not be longer than two months starting from the warrant, without prejudice to a renewal, and if applicable, the period in the past to which the warrant extends in accordance with paragraph 2.

---

[153] Annex 2 provides the future version of Article 88*bis* CCP.

> In case of *flagrante delicto*, the public prosecutor can order the measure for the offences provided in Article 90ter, §§2, 3 and 4 [linguistic reformulation in future law but without any change in content: "*In case of flagrante delicto, the public prosecutor can order the* measure for the offences enumerated in Article 90*ter*, §§2, 3 and 4"]. In this case, the investigating judge must confirm the measure within twenty-four hours. However, if it concerns an offense referred to in Article 347*bis* [taking of hostages] and 470 [extortion by force] of the Criminal Code, the public prosecutor can order the measure during the situation *flagrante delicto*, without requirement of confirmation by the investigating judge.
>
> The public prosecutor can order the measure upon request of the complainant, if the measure seems essential for establishing an offense referred to in Article 145 §3 and §3a of the Electronic Communications Act of 13 June 2005.[154]
>
> In cases of emergency, the measure can be ordered orally. The measure must be confirmed as soon as possible in the form set out in the third and fourth paragraphs.

bb) Duty of addressees to disclose information in manual procedures

Article 88*bis* §4 CCP reads as follows:

> §4. Any operator of an electronic communications network and any provider of an electronic communication service shall communicate the requested data within a period to be determined by the King, on the proposal of the Minister of Justice and the Minister responsible for Telecommunications.
>
> Any person, who by virtue of his office is informed of the action or cooperates thereto, is bound to secrecy. Any breach of secrecy is punishable in accordance with Article 458 of the Criminal Code.
>
> Any person who refuses technical cooperation with the request mentioned in this article, of which the King determines the modalities, shall be punished with a fine of twenty-six euro to ten thousand euros, on the proposal of the Minister of Justice and the Minister responsible for Telecommunications.

The modalities of the cooperation duties under Article 88*bis* CCP are laid down in the Royal Decree of 9 January 2003 regarding the legal duty to cooperate with judicial requests regarding electronic communications.[155] Article 4 of the Royal Decree provides that the traffic data of telecommunications, meaning from where or to where calls are or were made and that are more than 30 days old, shall be provided as soon as they are available and, at the latest, on the next working day at the same hour as the receipt of the request, unless the request provides otherwise.

---

[154] Article 145 §3, 1° of the Law of 13 June 2005 on electronic communications punishes anyone who carries out fraudulent electronic communications through a network of electronic communication in order to gain for himself/herself or another an unlawful advantage; Article 145 §3*bis* of the Law of 13 June 2005 on electronic communications incriminates "the person who uses an electronic communications network or an electronic communications service or other electronic means to annoy or cause damage to his correspondent and the person installing any device intended to commit the offence and the attempt to commit it."

[155] Royal Decree of 9 January 2003 regarding the legal duty to cooperate with judicial requests regarding electronic communications, *Belgian Official Journal*, 10 February 2003.

No automated procedure is prescribed for data transfers under Article 88*bis* CCP.

We refer to our earlier discussion regarding the duties to provide a technical and organizational infrastructure (section III.B.5.c.), the security requirements for data transfers by communication service providers (section III.B.5.d.) as well as checks, filtering, and decryption obligations of communication service providers (section III.B.5.e.).

### *b) Collection of subscriber data*

#### aa) Relevant information

Article 46*bis* CCP is on the collection of identification data of electronic communications. Article 46*bis*, §1, 1° and 2° CCP describes the relevant information:

> 1) the identification of the subscriber or the habitual user of an electronic communications service or of the used electronic communication means;
>
> 2) the identification of electronic communications services to which a particular person is a subscriber or that are habitually used by a particular person. The reasoning reflects the proportionality in relation to the privacy and the subsidiarity in relation to any other investigatory act.

#### bb) Substantive prerequisites of collection

##### (1) Degree of suspicion

According to Article 46*bis* §1 CCP, the public prosecutor may proceed or initiate to proceed with the collection of identification data of electronic communications "on the basis of any information in his possession".

##### (2) Predicate offenses

Article 46*bis* CCP does not contain a list of offenses that can justify a monitoring measure. According to Article 46*bis* §1 CCP, the measure can only be ordered for crimes and misdemeanours; hence, *a contrario*, not for contraventions.

##### (3) Persons and connections under surveillance

Article 46*bis* §1, 1° CCP refers to "the subscriber or the habitual user of an electronic communications service or of the used electronic communication means."

Article 46*bis* §1, 2° CCP refers to "electronic communications services to which a particular person is a subscriber or that are habitually used by a particular person."

(4) Principle of subsidiarity

Article 46*bis* §1, 2° CCP provides that the reasoning of the public prosecutor reflects the proportionality in relation to privacy and the subsidiarity in relation to any other investigatory act.

(5) Proportionality of interception in individual cases

Article 46*bis* §1, 2° CCP provides that the reasoning reflects the proportionality in relation to privacy and the subsidiarity in relation to any other investigatory act.

(6) Consent by a communication participant to the measure

As said earlier (section III.B.6.b.), according to Article 61*quinquies* §3 CCP, the judge may reject the request by the suspect or a civil party if he considers the measures unnecessary in order to reveal the truth or if, at that moment, he considers the measures prejudicial to the investigation.

cc) Formal prerequisites of collection

(1) Competent authorities

Under normal circumstances, the public prosecutor authorizes the measure (Article 46*bis* §1, 3° CCP).

Under circumstances of emergency, also a judicial police officer can authorize the measure, but only after consent of the public prosecutor. Article 46*bis* §2 CCP reads as follows:

> [i]n cases of extreme urgency, any judicial police officer can, after verbal and prior consent of the public prosecutor, in a reasoned and written decision order the production of these data.

(2) Formal requirements for applications

As said earlier (section III.B.6.b.), according to Article 61*quinquies* §3 CCP, the judge may reject the request by the suspect or a civil party if he considers the measures unnecessary in order to reveal the truth or if, at that moment, he considers the measures prejudicial to the investigation.

(3) Formal requirements for orders

Article 46*bis* §1 CCP provides that the public prosecutor issues a reasoned and written decision in order to proceed or initiate to proceed with the collection of identification data.

The Data Retention Act of 29 May 2016 added a new paragraph to Article 46*bis* §1 CCP:

> For criminal facts that cannot result in the imposition of a correctional penalty of one-year imprisonment or of a more severe penalty, the public prosecutor – or in case of extreme emergency, the judicial police officer – can only request the data referred to in the first paragraph, for a period of six months prior to its decision.

### dd) Duty of addressees to disclose information

Article 46*bis* §2 CCP reads as follows:

> §2. Any operator of an electronic communications network and any provider of an electronic communications service that is required to communicate information referred to in paragraph 1, provides the public prosecutor or judicial police officer the data that were requested within a period to be determined by the King, on the proposal of the Minister of Justice and the Minister competent for Telecommunications.
>
> The King determines, upon advice of the Privacy Commission and based on the proposal of the Minister of Justice and the Minister competent for Telecommunications, the technical conditions for the access to the information referred to in §1, which is available to the public prosecutor and to the police services designated in the same paragraph.
>
> Any person, who by virtue of his office is informed of the measure or cooperates thereto, is bound by secrecy. Any breach of secrecy shall be punished in accordance with Article 458 of the Criminal Code.
>
> Refusal to disclose the information shall be punished with a fine of twenty-six euro to ten thousand euros.

Of note in this regard is a judgment of the Belgian Supreme Court of 18 January 2011, in which the court gave an autonomous interpretation of the term "electronic communications provider" as mentioned in Article 46*bis* CCP (the collection of identification data of electronic communications). The Supreme Court held that:

> the obligation to cooperate under article 46bis of the Code of Criminal Procedure is not restricted to operators of an electronic communications network or to providers of an electronic communications service that are also operators within the meaning of the Electronic Communications Act of 13 June 2005, or that only provide their electronic communications services through their own infrastructure. This obligation also applies to anyone who provides a service, which consists wholly, or mainly in the conveyance of signals on electronic communications networks. The person who provides a service which consists of enabling its customers to obtain, or to receive or distribute information through an electronic network, can also be a provider of an electronic communications service.[156]

---

[156] Supreme Court, 18 January 2011, P.10.1347.N, available via http://jure.juridat.just.fgov.be/

ee) Automated procedure of disclosure

The modalities of the cooperation duties under Article 46*bis* CCP are laid down in the Royal Decree of 9 January 2003 regarding the legal duty to cooperate with judicial requests regarding electronic communications.[157]

Article 3 §1 of the Royal Decree provides that the Coordination Cell Justice of the operators of electronic communications networks that were not granted numbering capacity in the national numbering plan by the Belgian Institute for Postal Services and Telecommunications (BIPT),[158] and the electronic communications providers shall communicate in real time according to the rules provided in Article 10*bis* of the same Royal Decree (see section III.B.5.d. and e.).

Article 3 §2 of the Royal Decree prescribes an automated procedure of disclosure for electronic communications networks that were granted numbering capacity in the national numbering plan by the BIPT. The access is granted via a secure Internet application, by means of which the operator receives a request, which he is required to process and reply to immediately. The National Technical & Tactical Support Unit – Central Technical Interception Facility (NTSU-CTIF) determines further technical details of the procedure and shall only consult the database after receipt of a request based on Article 46*bis* CCP. The NTSU-CTIF shall keep a log file of every access to and consultation of the database and take the necessary physical and software-based measures in order to install an adequate security level.

In addition, we refer to our earlier discussion about the duties to provide a technical and organizational infrastructure (section III.B.5.c.), the security requirements for data transfers by communication service providers (section III.B.5.d.) as well as checks, filtering, and decryption obligations of communication service providers (section III.B.5.e.).

*c) Data retention*[159]

As said earlier (section I.A.2.a.dd.), the general data retention (preservation) provision is Article 126 of the Electronic Communications Act.[160] However, on

---

[157] Royal decree of 9 January 2003 regarding the legal duty to cooperate with judicial requests regarding electronic communications, *Belgian Official Journal,* 10 February 2003.

[158] On the basis of Article 11 §1 of the Electronic Communications Act of 13 June 2005.

[159] For further details, see the authors' country report for the Cybercrime Research Centre at Nicolaus Copernicus University (Poland): Paul De Hert and Gertjan Boulet, "The cooperation between Internet service/access providers and law enforcement authorities," February 2015, 29 pp., available at http://www.cybercrime.umk.pl/files/files/Report%20Belgium_De%20Hert%20Boulet.docx

[160] As amended by the Belgian Communication Act of 30 July 2013 amending Articles 2, 126, and 145 of the Act of 13 June 2005 on electronic communications and Article

11 June 2015, the Belgian Constitutional Court invalidated Article 126 of the Electronic Communications Act.[161] A new Belgian data retention law of 29 May 2016 entered into force on 28 July 2016.

Article 126 §1 of the Electronic Communications Act of 13 June 2005 provided that the following providers of *publicly available* services are subject to data retention obligations:

- Landline telephony services;
- Mobile telephony services;
- Internet access services;
- Internet e-mail services;
- Internet telephony services;
- Providers of underlying public electronic communication networks;
- Resellers in own name and on own behalf.

The Data Retention Act of 29 May 2016 retains these categories in the new version of Article 126, with the exception of resellers in own name and on own behalf.

The former version of Article 126 §3 of the Electronic Communications Act of 13 June 2005 established a data retention period of 12 months. The former version of Article 126 §4 of the Electronic Communications Act provided that the King could extend the data retention periods for certain categories of data, without exceeding 18 months, as well as install a temporary data retention period of more than 12 months. If the data retention period in the latter case exceeded 24 months, then the minister competent for telecommunications could inform the other EU Member States and the European Commission (EC).

The Data Retention Act of 29 May 2016 deletes paragraph 4 of Article 126 and lays down a uniform data retention period of 12 months in Article 126 §3, without the possibility of renewal.

The new version of Article 126 Data Retention Act of the Electronic Communications Act 29 May 2016 retains the requirement that the following statistics shall be added to the annual reports of the Minister of Justice in implementation of Article 90*decies* CCP:

1° the cases in which data have been provided to the competent authorities in accordance with the applicable legal provisions;

2° the time elapsed between the date on which the data were retained and the date on which the competent authority requested the transfer;

3° the cases in which the data requests could not be met.

---

90*decies* of the Code of Criminal Procedure, *Belgian Official Journal*, 23 August 2013, entry into force on 2 September 2013.

[161] Constitutional Court of Belgium, 11 June 2015, no. 84/2015, available at http://www.const-court.be/public/n/2015/2015-084n.pdf

A Royal Decree of 19 September 2013 lists the types of data that are subject to data retention.[162]

Article 3 §1 of the Royal Decree of 19 September 2013 provides that landline telephony services retain the following identification data:

1) the number allocated to the user;
2) the user's personal data;
3) the subscription's starting date or the registration data;
4) the type of landline telephony service used and the types of other services with which the user is registered;
5) in case of number transfer, the identity of the transferring provider and of the receiving provider;
6) the data relating to the payment method, the identification of the payment instrument, and the time of payment for the subscription or for the use of the service.

Article 3 §2 of the Royal Decree of 19 September 2013 provides that landline telephony services retain the following traffic and localization data:

1) the identification of the calling number and the number called;
2) the location of the network connection point of the calling party and of the called party;
3) the identification of all lines in case of group calls, call forwarding, or call transfer;
4) data and time of the start and end of the call;
5) description of the telephony service used.

Article 4 §1 of the Royal Decree of 19 September 2013 provides that mobile telephony services retain the following identification data:

1) the number allocated to the user and his International Mobile Subscriber Identity (IMSI);
2) the user's personal data;
3) the date and location of the user's registration or subscription;
4) the date and time of the first activation of the service and the cell ID from which the service is activated;
5) the additional services to which the user has subscribed;
6) in case of number transfer, the identity of the transferring provider;

---

[162] Royal Decree of 19 September 2013 regarding the execution of Article 126 of the Act of 13 June 2005 on electronic communications, *Belgian Official Journal*, 8 October 2013, entry into force on 19 September 2013.

7) the data relating to the payment method, the identification of the payment instrument, and the time of payment for the subscription or for the use of the service;
8) the ID number of the user's mobile equipment (IMEI).

Article 4 §2 of the Royal Decree of 19 September 2013 provides that mobile telephony services retain the following traffic and localization data:

1) the identification of the telephone number of the calling party and of the called party;
2) the identification of all lines in case of group calls, call forwarding, or call transfer;
3) the IMSI of the calling and called participants;
4) the IMEI of the mobile equipment of the calling and called participants;
5) the data and time of the start and end of the call;
6) the location of the network connection point at the start and the end of each connection;
7) the identification of the geographic location of cells, via reference to the cell ID, at the time of connection;
8) the technical characteristics of the telephony service used.

Article 5 §1 of the Royal Decree of 19 September 2013 provides that Internet access services retain the following identification data:

1) the user ID allocated;
2) the user's personal data;
3) the data and time of the user's registration or subscription;
4) the IP-address, source port of the connection used for subscribing or registering the user;
5) the identification of the network connection point used for subscribing or registering the user;
6) the additional services to which the user has subscribed with the provider concerned;
7) the data relating to the payment method, identification of the payment instrument, and the time of payment of the subscription fee or for the use of the service.

Article 5 §2 of the Royal Decree of 19 September 2013 provides that Internet access services retain the following traffic and localization data:

1) the user's ID;
2a) the IP-address;
2b) in case of shared use of an IP-address, the ports allocated to the IP-address and the data and time of allocation;

3) the identification and location of the network connection point used when logging-in and logging-off;
4) the data and time of an Internet access service session's log-in and log-off;
5) the data volume uploaded and downloaded during a session;
6) the data necessary to identify the geographic location of cells, via reference to the cell ID, at the time of the connection.

Article 6 §1 of the Royal Decree of 19 September 2013 provides that Internet e-mail services and Internet telephony services retain the following identification data:

1) the user ID;
2) the user's personal data;
3) the data and time of creation of the e-mail or Internet telephony account;
4) the IP-address and source port used for the creation of the e-mail or Internet telephony account;
5) the data relating to the payment method, the identification of the payment instrument, and the time of payment of the subscription fee or for the use of the service.

Article 6 §2 of the Royal Decree of 19 September 2013 provides that Internet e-mail services and Internet telephony services retain the following traffic and localization data:

1) the user's ID relating to the e-mail or Internet telephony account, including the number of the ID code of the intended recipient of the communication;
2) the telephony number allocated to each communication entering the telephony network within the framework of an Internet telephony service;
3a) the IP-address and the source port used by the user;
3b) the IP-address and the source port used by the addressee;
4) the data and time of the log-in and log-off of a session of the e-mail service or Internet telephony service;
5) the data and time of a connection made by means of the Internet telephony account;
6) the technical characteristics of the service used.

Article 9 §7 of the Electronic Communications Act of 13 June 2005 provides that a specific Royal Decree shall address the matter of data retention for closed user groups. Federal Magistrate Jan Kerkhofs and Investigating Judge Philippe Van Linthout state that it could be said that Belgian providers of electronic communication services or networks with no notification duty are currently released from data

retention obligations, taking into account the lack of a specific Royal Decree.[163] For the same reason, service providers that act as a mere conduit or provide caching and hosting activities under the Code of Economic Law are currently released from data retention obligations.

Ultimately, it should be noted that notaries, bailiffsn and accountants are subject to specific data retention and production obligations, provided in Article 7 and under chapter III of the Law of 11 January 1993 on preventing misuse of the financial system for purposes of laundering money and terrorism financing).[164]

## 2. Identification of device ID (IMEI), card number (IMSI), and location of mobile terminal devices

### *a) Identification of IMEI and IMSI*

The Belgian CCP does not have a specific provision for the identification of the device ID (IMEI)[165] and the card number (IMSI).[166] Kerkhofs and Van Linthout say that such identification activities are justified on the basis of Article 46*bis* CCP on the collection of identification data of electronic communications (see section III.C.1.).[167]

### *b) Location determination via "silent SMS"*

In a reply of 9 June 2011 to a parliamentary question regarding the use of "stealth" (silent SMS) technology, the Minister of Justice confirmed that such activities are justified on the basis of Article 88*bis* §1 CCP regarding the tracing of traffic data, and localization of electronic communications.[168]

---

[163] Jan Kerkhofs and Philippe Van Linthout, *Cybercrime*, Brussels, Politeia, 2013, p. 396.

[164] Act of 11 January 1993 on preventing misuse of the financial system for purposes of laundering money and terrorism financing, *Belgian Official Journal*, 9 February 1993, entry into force on 1 December 1993, available at http://www.imolin.org/doc/amlid/Belgium_law_11_January_1993.pdf

[165] International Mobile Station Equipment Identity.

[166] International Mobile Subscriber Identity.

[167] Jan Kerkhofs and Philippe Van Linthout, *Cybercrime*, Brussels, Politeia, 2013, p. 356.

[168] Belgian Chamber of Representatives, *Schriftelijke vragen en antwoorden* (Written questions and answers), 2010–2011, no. 53-032, pp. 35–36, available at http://www.dekamer.be/QRVA/pdf/53/53K0032.pdf; see also Jan Kerkhofs and Philippe Van Linthout, *Cybercrime*, Brussels, Politeia, 2013, p. 258.

## D. Access to (Temporarily) Stored Communication Data

### 1. Online searches with the help of remote forensic software

#### *a) Looking-in operations and observation*

As noted earlier (section III.B.4.b.), the use of "technical means" is allowed for the looking-in operations power (Articles 46*quinquies* and 89*ter* CCP) and observation power (Article 47*sexies* CCP).

The power of looking-in operations allows the public prosecutor to authorize police officers to enter a private place, without knowledge of the owner or consent of the owner, in case there are serious suspicions that the punishable acts constitute or would constitute a crime referred to in Article 90*ter* §§2–4 CCP (on wiretapping, see section III.B.7.b.), or are committed or would be committed in the context of a criminal organization as referred to in Article 324*bis* CC, and when no other investigation means suffice to reveal the truth. In case the private place is a home, a part of a home, or the office of a lawyer of doctor, then the investigating judge has to authorize the measure (Article 89*ter* CCP).

Kerkhofs and Van Linthout view private cyber areas as a private place in the meaning of Article 46*quinquies* §1 CCP.[169]

Article 46*quinquies* §2 CCP lays down the limited cases in which looking-in operations may be used:

1) to record the place and to assess the potential presence of goods that are the object of the crime, or that were used to commit the crime, or that result from the crime, or of the presence of profits gained from committing the crime;
2) to collect evidence of the presence of those items;
3) to install technical means within the framework of the observation power (Article 47*sexies* CCP).

In the latter case, the authorization of the looking-in operation and all official reports shall be added to the judicial file at the latest after completion of the observation (see Article 46*quinquies* §1 *in fine* CCP). The suspect has access to the judicial file (Article 61*ter* CCP).

The observation power empowers the public prosecutor and the investigating judge to order systematic observation by police officers of one or more persons, their presence or behavior, or of certain items, places, or events. An observation is systematic when:

1) it is longer than five consecutive days or five non-consecutive days within a period of a month;

---

[169] Jan Kerkhofs and Philippe Van Linthout, *Cybercrime*, Brussels, Politeia, 2013, pp. 242–243.

2) it involves the use of technical means;
3) it has an international character;
4) it is performed by special units of the federal police.

The authorization of the observation and all official reports shall be added to the judicial file at the latest after completion of the observation (Article 47*septies* CCP).

The term "technical means" appears twice in Article 46*quinquies* CCP. First, Article 46*quinquies* §2, 3° CCP mentions the use of looking-in operations to install technical means within the framework of the observation power (Article 47*sexies* CCP) and refers to the meaning of the term technical means provided in Article 47*sexies* §1, 3° (observation):

> technical means is a configuration of components that detects and transmits signals, activates their recording and records the signals, with the exception of technical means used to perform a measure under Article 90ter [CCP].

Hence, the meaning of the term technical means in relation to the observation power is not identical to the meaning of the same term in Article 90*ter* §1, 2° (see section III.B.4.b.). In fact, microphones are a traditional example of technical means that can be used for the eavesdropping measure but not for the looking-in operation and observation.[170] Bockstaele, Chief Commissioner with the Ghent judicial police, gives as examples of technical means for the observation measure: a video camera, motion detectors, or a tracking system[171] on a container.[172]

Second, Article 46*quinquies* §4 CCP mentions the use of technical means for *all* purposes provided in Article 46*quinquies* §2 CCP, thus not only for the purpose to use the observation power (see section III.D.1.). The parliamentary preparatory works explain that this category is actually unlimited, including an infrared camera, an endoscope, and a drill to make a hole in the roof.[173]

For Kerkhofs and Van Linthout, technical means include key loggers, cameras, spyware, hacking, etc.[174] Legal doctrine, however, questions the extraterritorial scope of these powers, considering the significant cross-border reach of technical

---

[170] Christine Van den Wyngaert, (An Outline of Criminal Law, Criminal Procedural Law & International Criminal Law), Antwerp-Apeldoorn, Maklu, 2006, pp. 963, 982 and 991.

[171] Peilzender (in Dutch).

[172] Marc Bockstaele and others (eds.), *De Zoeking onderzocht* (An analysis of the search), Antwerp-Apeldoorn, Maklu, 2009, p. 87.

[173] Parliamentary preparatory works, Belgian Chamber of Representatives, regarding the special investigation methods and any other methods of investigation, 2001-2002, no. 50 1688/001, pp. 87–88, available via http://www.senate.be/www/?MIval=dossier&LEG=2&NR=1260&LANG=nl

[174] Jan Kerkhofs and Philippe Van Linthout, *Cybercrime*, Brussels, Politeia, 2013, pp. 241, 243.

means, such as botnet crawlers, i.e., a technique "used for gathering intelligence on a P2P botnet, a decentralized network of infected computers under the control of a bot master".[175]

### *b) Network search*

Article 88*ter* CCP referts to the network search, which empowers the investigating judge, when ordering the search of a computer system or a part thereof, to expand this search to a computer system or a part thereof at a place other than where the search takes place:

> §1. When the investigating judge orders a search in a computer system or part therefore, this search can be expanded to a computer system or a part thereof at a place other than where the search takes place:
> – If such expansion is necessary to reveal the truth concerning the investigated offense which is the object of the search; and
> – If other measures would be disproportional, or if there is a risk that without such expansion evidence would be lost.
>
> §2. The expansion of the search in an information system may not extend further than to information systems or the parts to which the persons that have the rights to use the searched information system, have specific access.
>
> §3. Regarding the data gathered by expanding the search in an information system, and that are useful for the same purposes as the seizure, one shall operate as specified in Article 39bis. The investigating judge shall inform the responsible of this computer system, unless his identity or domicile cannot be reasonably found.
>
> If it appears that these data are not situated on the national territory, then only copying is allowed. In that case, the investigating judge shall promptly notify, through the public prosecutor, the Minister of Justice, who will subsequently notify the competent authority of the State concerned, if it can be reasonably determined.
>
> §4. Article 89bis [on the designation of judicial police officers for the home search and seizure] applies to the expansion of the search in a computer system.

Conings and Oerlemans say that the use of hacker tools seems possible when the investigating judge does not have access to the computer system, and that the use of these tools would not violate the prohibition of hacking provided in Article 550*bis* CC.[176]

---

[175] Karine Silva and Ruben Roex, "Zombie alert: Assessing legitimacy of P2P botnet mitigation techniques," 2014, conference paper, 25th European Regional Conference of the International Telecommunications Society (ITS), Brussels, Belgium, 22–25 June 2014, p. 1, available at http://econstor.eu/bitstream/10419/101402/1/795035411.pdf

[176] Charlotte Konings and Jaap-Jan Oerlemans, "Van een netwerkzoeking naar online doorzoeking: grenzeloos of grensverleggend" (From a network search to an online search: borderless or groundbreaking?), *Computerrecht*, 2013, vol. 5, pp. 23–32, available at https://www.b-ccentre.be/download/b-ccentre_legal/B-CCENTRE%20Van%20een%20netwerkzoeking%20naar%20online%20doorzoeking.pdf

## 2. Search and seizure of stored communication data

### *a) Special provisions*

The CCP contains a specific provision for data seizure, but not for the search of stored communication data. Article 39*bis* CCP is on data seizure and reads as follows:

> §1. Without prejudice to specific provisions of this Article, the rules in this Code on the seizure, including Article 28 sexies, apply to the copying, making inaccessible and deleting data stored in a computer system.
>
> §2. If the public prosecutor or the labour prosecutor encounters stored data in a computer system that are useful for the same purposes as the seizure, but when the seizure of their carrier is not desirable, these data and the data necessary for reading them, are copied on carriers belonging to the government. In case of urgency or for technical reasons, use can be made of carriers, which are available to persons who are entitled to use the computer system.
>
> §3. He uses the appropriate technical means to prevent the access to and to guarantee the integrity of these data in the computer system, as well as the copies thereof which are available to persons who are entitled to use the computer system.
>
> If the data are the subject of the offence or have been produced by the offence and if they infringe public order or public decency or constitute a danger to the integrity of computer systems or data stored, processed or transmitted through such system, the public prosecutor or the labour prosecutor shall use all appropriate technical means to make these data inaccessible.
>
> Except in the case referred to in the preceding paragraph, he may, however, allow the further use of all or part of these data, when it does not endanger the prosecution.
>
> §4. If the measure specified in §2 is not possible for technical reasons or because of the size of the data, he uses the appropriate technical means to prevent the access to the data and to guarantee the integrity of these data in the computer system, as well as the copies thereof which are available to persons who are entitled to use the computer system.
>
> §5. The public prosecutor or the labour prosecutor informs the responsible of the computer system of the search in the computer system, and communicates to him a summary of the data copied, made inaccessible or deleted.
>
> §6. The public prosecutor or the Labour prosecutor uses the appropriate technical means to ensure the integrity and confidentiality of the data.
>
> Appropriate technical resources are used for the preservation of these data on the Registry.
>
> The same applies if data stored, processed or transmitted through a computer system, are seized along with their carrier, pursuant to the previous articles.

### *b) Applicability of seizure provisions to electronic data*

The foregoing shows that the data seizure (Article 39*bis* CCP) applies to electronic data. A current matter of dispute, however, is to what extent this data "seizure" power also includes information "search" powers.

Konings and Oerlemans distinguish the network search (Article 88*ter* CCP) from both the online search and the information search (search of stored communication data).[177] Moreover, they find that Belgian law does not contain any legal basis at all for the latter two investigation methods.

Regarding the online search, Belgian law enforcement agencies do access the cloud on the basis of the network search.[178]

Regarding the information search, Kerkhofs and Van Linthout read this power in the (data) seizure provisions (Article 35 CCP, Article 39*bis* CCP, etc.).[179] Their view was echoed by the Supreme Court in its judgment of 11 February 2015, in which it held that the data seizure from a mobile (Article 39*bis* CCP) empowers the police officers to analyze the data stored in the information memory. The Court referred to Article 35 CCP (the standard seizure provision) and Article 39*bis* §2 CCP (the data seizure provision): the latter article provides that the public prosecutor can copy stored data on a computer system if these data are useful for the same purposes as the seizure and if the seizure of the data carrier is not desirable.

Hence, the information search is covered by the seizure provision of Article 39*bis* CCP rather than by the general monitoring measure (Article 90*ter* CCP) or the other investigation methods to access stored communication data: looking-in operations (Article 46*quinquies* CCP), observation (Article 47*sexies* CCP), and the network search (Article 88*ter* CCP).

However, the Supreme Court held that, for data access to the cloud, the power of the network search (Article 88*ter* CCP) needs to be applied.[180] As noted earlier (section III.B.2.c.), webmail that arrives in an online web mailbox is deemed out of transmission and therefore can no longer be intercepted on the basis of Article 90*ter* CCP. In these cases, only a network search is possible (Article 88*ter* CCP) or a data seizure (Article 39*ter* CCP). However, it is debated whether or not pop-mail arriving in an online web mailbox is still deemed to be in transmission and therefore whether or not it could be intercepted on the basis of Article 90*ter* CCP.

---

177 Charlotte Konings and Jaap-Jan Oerlemans, "Van een netwerkzoeking naar online doorzoeking: grenzeloos of grensverleggend" (From a network search to an online search: borderless or groundbreaking?), *Computerrecht*, 2013, vol. 5, pp. 23-32, available at https://www.b-ccentre.be/download/b-ccentre_legal/B-CCENTRE%20Van%20een%20netwerkzoeking%20naar%20online%20doorzoeking.pdf. On the network search, see section III.D.1.

178 Jan Kerkhofs and Philippe Van Linthout, *Cybercrime*, Brussels, Politeia, 2013, pp. 263, 268 and 295.

179 Jan Kerkhofs and Philippe Van Linthout, *Cybercrime*, Brussels, Politeia, 2013, p. 167.

180 Supreme Court, 11 February 2015, P.14.1739.F, available at http://www.legalworld.be/legalworld/uploadedFiles/Rechtspraak/De_Juristenkrant/P.14.1739.F%20(11.02.2015)%20(gsm%20-%20pdk).pdf?LangType=2067

*c) Different standards of protection for stored and for transmitted data*

As noted earlier (sections II.A.4.a. and III.B.10.c.), the monitoring measure in Article 90*ter* CCP provides an exception to the general prohibition of the interception of (tele-)communications provided in Article 314*bis* and Article 259*bis* CC. Article 314*bis* CC lays down the prohibition, applicable to everyone, of taking cognizance of the contents of a telecommunication one does not participate in *during the transfer* of the telecommunication. A similar prohibition was introduced for public officials in Article 259*bis* CC. Hence, the standards provided in Article 90*ter* CCP for interception data in transmission are higher than the standards for accessing stored data on the basis of other provisions.

*d) Open and clandestine access to stored data*

Article 39*bis* §5 CCP provides that "[t]he public prosecutor or the labour prosecutor informs the responsible of the computer system of the search in the computer system, and communicates to him a summary of the data copied, made inaccessible or deleted".

### 3. Duties to cooperate: production and decryption orders

As noted (sections I.A.2.a., III.B.5., III.C.1.), the CCP contains production and decryption orders in connection with the collection of identification data of electronic communications (Article 46*bis* CCP), tracing of traffic data, and localization of electronic communications (Article 88*bis* CCP), the network search (Article 88*ter* CCP), and wiretapping (Article 90*ter* CCP).

With regard to Article 46*bis*, Article 88*bis*, and Article 90*ter* CCP, the fourth functional requirement in Article 6 §1 of the Royal Decree of 9 January 2003 concerns the transfer of content of data in plain language in case the operator of an electronic communications network or the provider of electronic communications introduced encoding, compression, or encryption of the electronic communications traffic.

With regard to Article 88*ter* CCP, Article 88*quater* §1 CCP reads as follows:

> §1. The investigating judge, or on his behalf a judicial police officer, assistant officer of the public prosecutor and of the labour prosecutor, can order persons of whom the investigating judge thinks that they have special knowledge concerning the computer system that is the object of a search, or of services to protect or encrypt data that are processed, encrypted or transferred through a computer system, to provide information concerning its functioning or the ways to get access to it, or to get access in an understandable format to the data that are processed, encrypted or transferred through it. The investigating judge specifies the factual circumstances of the case that justify the measure in a substantiated warrant that he communicates to the public prosecutor or the labour prosecutor.

All these cooperation duties also apply to the suspect, with the exception of the specific cooperation duty laid down in Article 88*quater* §2 CCP in relation to the network search:

> §2. The investigating judge, or on his behalf a judicial police officer, assistant officer of the public prosecutor and of the labour prosecutor, can order any suitable person to operate the computer system himself or, as appropriate, to search, to make accessible, to copy, to make inaccessible or to delete the relevant data that are processed, encrypted or transferred through it. These persons are obliged to comply with the order, to the extent of their capabilities.
>
> The order referred to in the first paragraph cannot be given to the accused and to the persons referred to in Article 156.

Kerkhofs and Van Linthout explain that, whereas Article 88*quater* §2 CCP concerns actions to be taken by the suspect, the other articles concern the provision of mere intelligence or existing evidence. They refer to the case *Saunders v. the United Kingdom* in which the ECtHR held that:

> [t]he right not to incriminate oneself, in particular, presupposes that the prosecution in a criminal case seek to prove their case against the accused without resort to evidence obtained through methods of coercion or oppression in defiance of the will of the accused.[181]

Thus, Kerkhofs and Van Linthout accept the practice of requesting cooperation from suspects.

Yet, they add as a side remark that it is still to be seen whether this solution will pass the human rights test by the ECtHR.[182]

Article 39*bis* CCP does not lay down production and decryption orders. However, Article 39*bis* §3 CCP allows the public prosecutor to order the seizure of alleged illegal data (e.g., a computer virus). The public prosecutor can use all technical means to make data inaccessible that:

> are the subject of the offence or have been produced by the offence and if they infringe public order or public decency or constitute a danger to the integrity of computer systems or data stored, processed or transmitted through such system.

This power is used, for example, by prosecutors to request an Internet Service Provider (ISP) to delete from their Domain Name Server (DNS) the domain name of a site that violates the law.

---

[181] ECtHR, *Saunders v. the United Kingdom*, Grand Chamber, 17 December 1996, No. 19187/91, §68, available via http://hudoc.echr.coe.int/

[182] Jan Kerkhofs and Philippe Van Linthout, *Cybercrime*, Brussels, Politeia, 2013, p. 369.

# IV. Use of Electronic Communication Data in Judicial Proceedings

## 1. Use of electronic communication data in the law of criminal procedure

There are no rules specifically designed for using intercepted or stored electronic data as evidence in court proceedings.

In Belgium, the use of evidence is free. Hence there are no limits regarding the form by which intercepted material shall be introduced as evidence in criminal proceedings.[183]

## 2. Inadmissibility of evidence as a consequence of inappropriate collection

In Belgium, illegally obtained evidence follows from:

1) the commission of a criminal offense;
2) a violation of the law of criminal procedure;
3) a violation of the right to privacy;
4) a violation of the right of defense;
5) a violation of the right to human dignity.[184]

However, an illegality committed during evidence collection does not automatically result in the exclusion of the illegally obtained evidence. In its judgment of 14 October 2003, the Supreme Court developed three exclusionary rules, the so-called Antigoon criteria for excluding illegally obtained evidence.[185] More particularly, evidence has to be excluded in three cases:

1) if compliance with procedural rules is legally prescribed under penalty of nullity;
2) if the illegality has compromised the reliability of the evidence;
3) if the use of the illegally obtained evidence violates the right to a fair trial.

In a judgment of 23 March 2004,[186] the Supreme Court held that the violation of the right to a fair trial has to be assessed on the basis of all aspects of the case as a whole, and proposed a number of factors that the judge can take into consideration:

---

[183] Raf Verstraeten, *Handboek strafvordering* (Manual on criminal procedure), Antwerp, Maklu, 2007, p. 859; Chris Van den Wyngaert, *Strafrecht, Strafprocesrecht & Internationaal Strafrecht in hoofdlijnen* (An Outline of Criminal Law, Criminal Procedural Law & International Criminal Law), Antwerp-Apeldoorn, Maklu, 2006, p. 1127.

[184] Raf Verstraeten and Frank Verbruggen, *Straf- en strafprocesrecht voor bachelors* (Criminal law and criminal procedural law for bachelors), Antwerp-Apeldoorn, Maklu, 2007, p. 336.

[185] Supreme Court, 14 October 2003, P030762N, available via http://jure.juridat.just.fgov.be/

[186] Supreme Court, 23 March 2004, P040012N, available via http://jure.juridat.just.fgov.be/

1) whether or not the authorities intentionally committed the illegality;
2) whether the seriousness of the criminal offense exceeds the seriousness of the illegality committed;
3) whether or not the illegality only concerns a material element of the criminal offense;
4) the impact of the illegality on the protected fundamental right;
5) the mere formal nature of the illegality.

The Act of 24 October 2013[187] laid down the Antigoon exclusionary rules in Article 32 of the Preliminary Title of the CCP. However, the Belgian legislator did not incorporate a fourth exclusionary rule developed by the Supreme Court in a judgment of 26 January 2011: an illegality that concerns "a substantial procedural rule that affects the organization of the courts," i.e., an illegality concerning the *material* jurisdiction of the courts.[188] The Supreme Court held that this fourth exclusionary rule does not apply if the illegality concerns the *territorial* jurisdiction of the courts: in this case, exclusion of evidence can only be based on the three traditional Antigoon criteria. In a judgment of 24 April 2013, the Supreme Court effectively applied the fourth exclusionary rule to evidence found during a home search[189] that was authorized by a judge in a police court instead of by the investigating judge.[190]

Regarding the investigation methods referred to in this report, only the formal requirements for monitoring measures (Article 90*quater* §1 CCP) are prescribed under sanction of nullity (see section III.B.6.b. above):

§1 The investigating judge authorizes each monitoring measure under Article 90ter by a reasoned decision, and communicates the warrant to the public prosecutor.

On penalty of nullity, the warrant shall be dated and mentions:

1° the indications and concrete facts specific to the case, which justify the measure under Article 90ter;

2° the reasons why the measure is necessary to reveal the truth;

3° the person, the (tele-)communications method or the place that is the subject of the monitoring measure;

---

[187] Act of 24 October 2013 amending the Preliminary Title of the Code of Criminal Procedure, *Belgian Official Journal*, 12 November 2013, entry into force on 22 November 2013.

[188] Supreme Court, 26 January 2011, P.10.1321.F, available via http://jure.juridat.just.fgov.be/ ; See also the report of the law firm Eubelius: "Legal Embedment of the Antigoon case law", December 2013, available at http://www.eubelius.be/en/spotlight/legal-embedment-antigoon-case-law

[189] On the basis of the Act of 16 November 1972 concerning the Labour Inspectorate, *Belgian Official Journal,* 8 December 1972, entry into force on the same date.

[190] Supreme Court, 24 April 2013, P.12.1919.F.

4° the period during which the monitoring measure can be carried out, which should not be longer than one month counting from the decision by which the measure is ordered;

5° the name and the capacity of the judicial police officer designated for the implementation of the measure.

Regarding Article 90*quater* §1n 5° CCP, i.e., the duty to mention in the warrant the name and the capacity of the judicial police officer designated for the implementation of the measure, the Supreme Court held in a judgment of 19 June 1967 that another agent than the one mentioned in the warrant can implement the monitoring measure. In fact, implementation by the judicial police officer only concerns a measure of implementation of the warrant, not the legality of the warrant itself.[191]

As said earlier (section III.B.3.a.aa.), although notification of the Bar and the order of physicians for a monitoring measure that covers premises used for business purposes or domicile, or the (tele-)communications means of a lawyer or a doctor (Article 90*octies* §2 CCP), is not prescribed under sanction of nullity, the parliamentary preparatory works underline that the public order nature of this provision implies that failure to do so will entail the nullity of the monitoring measure.[192]

Apart from the exclusionary rules discussed above, the issue of "admissibility" emerges when a court potentially cannot admit evidence because its legality cannot be determined.[193] With regard to a foreign wiretapping measure, the Supreme Court held on 30 March 2010 that the non-availability of sufficient data to assess the legality of *one piece* of evidence can result in the non-admissibility of that piece; and that the non-availability of sufficient data to assess the legality of *all* evidence can result in the non-admissibility or the exclusion of the evidence but not in the discontinuance of the proceedings.[194]

On 3 April 2012, the Supreme Court found a violation of the right of defense, as the defense did not have the possibility to assess the legality of evidence resulting from a Dutch wiretapping measure: more specifically, the Court of Appeal of Antwerp had assessed the legality of the evidence merely on the basis of the evidence itself and a letter of the Dutch public prosecutor (officier van justitie).[195] The Su-

---

[191] Supreme Court, 19 June 1967, P.07.0311.

[192] Parliamentary preparatory works, regarding the legislative proposal protecting privacy against the interception of communication and telecommunication, Belgian Senate, 1993–1994, 18 May 1994, no. 843-2, p. 189, available at http://www.senate.be/lexdocs/S0539/S05390364.pdf

[193] Raf Verstraeten, *Handboek strafvordering* (Manual on criminal procedure), Antwerp, Maklu, 2012, p. 1015.

[194] Supreme Court, 30 March 2010, P.09.1789.N/1, available via http://jure.juridat.just.fgov.be/

[195] Supreme Court, 3 April 2012, P.10.0973.N, available via http://jure.juridat.just.fgov.be/

preme Court clarified that the assessment of the legality of the evidence can be based on the authorization of the wiretapping measure.

### 3. Use of data outside the main proceedings

#### *a) Data from other criminal investigations*

The judge does not have a right of injunction against the public prosecutor and thus cannot order the public prosecutor to request the judicial files of other criminal investigations.[196]

In this regard, it is of note that intercepted data can be used for the prosecution of individuals who were not the subject of the underlying interception order, but if so, only in another criminal investigation. Verstraeten and Verbruggen hold that the monitoring measure may not be halted if it reveals information pointing to the commission of offenses not anticipated by or not mentioned in the monitoring order.[197] These offenses are lawfully established only insofar as the execution of the monitoring measure does not exceed the limits of the authorization. The investigating judge cannot extend the investigation to these offenses if no action was brought before him/her in relation to these offenses. The investigating judge must inform the public prosecutor of these offenses on the basis of Article 56 §1 *in fine* CCP.

#### *b) Data from preventive investigations*

Data obtained from intelligence services and non-judicial police forces are admissible as evidence in criminal proceedings. We refer to our earlier discussion regarding the data exchanges between preventive police authorities/intelligence agencies and law enforcement authorities (section I.A.4.).

#### *c) Data obtained from foreign jurisdictions*

Article 6 of the Act of 9 December 2004 concerning international mutual legal assistance in criminal matters lays down the general rules on international legal assistance in criminal matters (see below, section V.A.3.).

---

[196] Court of Appeal of Antwerp, 13 March 2002, annotated by Bart De Smet, "Voeging van strafdossiers op verzoek van de verdediging" (Adding a file at the request of the defense), *Rechtskundig Weekblad*, 2002-2003, p. 1022; see Chris Van den Wyngaert, *Strafrecht, Strafprocesrecht & Internationaal Strafrecht in hoofdlijnen* (An Outline of Criminal Law, Criminal Procedural Law & International Criminal Law), Antwerp-Apeldoorn, Maklu, 2006, p. 615.

[197] Raf Verstraeten and Frank Verbruggen, *Straf- en strafprocesrecht voor bachelors* (Criminal law and criminal procedural law for bachelors), Antwerp-Apeldoorn, Maklu, 2007, pp. 209 and 220, nos. 873 and 933.

Article 13 of the Act of 9 December 2004 regarding mutual assistance in criminal matters[198] lays down the rules on the admissibility of intercepted data obtained from foreign jurisdictions. These rules match the Antigoon criteria discussed above (section IV.2.). Article 13 of the Act of 9 December 2004 reads as follows:

> Within the framework of criminal proceedings conducted before a Belgian court, no use shall be made of evidence:
>
> 1° which was illegally obtained in a foreign country if the illegality:
>
> – follows from the infringement of procedural requirements prescribed under sanction of nullity according to the law of the state where the evidence was obtained
>
> – compromises the reliability of the evidence;
>
> 2° of which the use would imply a violation of the fundamental right of a fair trial.

## 4. Challenging the probity of intercepted data

### *a) Duty to ensure the integrity and confidentiality of the recorded (tele-)communications*

Article 90*septies* §5 CCP provides that:

> [t]he appropriate means are used to ensure the integrity and confidentiality of the recorded (tele-)communications, and where possible, to ensure the transcription or translation. The same applies to the custody at the Registry of the records and the transcription or translation thereof, and to the entries in the special register. The King determines, after consulting the Privacy Commission, these means as well as the time when they replace the custody in a sealed envelope or the special register, referred to in the third and the fourth paragraph.

In relation to the data seizure measure (Article 39*bis* CCP), Kerkhofs and Van Linthout explain the need for regulating the chain of custody and for expert reports about the integrity of the evidence.[199] Similar concerns could arguably be raised regarding the integrity and reliability of intercepted data.

### *b) Access of parties to the judicial file*

Article 90*sexies in fine* CCP (monitoring measure) provides that:

> [t]he warrants of the investigating judge, the reports of the judicial police officers referred to in Article 90quater, §3, and the official records relating to the implementation of the measure, are included in the judicial file at the latest by the end of the measure.

The suspect has access to the judicial file (Article 61*ter* CCP). As said (section IV.2.), Article 90*quater* §1 CCP provides that the warrant shall mention:

---

[198] Act of 9 December 2004 regarding mutual assistance in criminal matters and modifying Article 90ter of the Code of Criminal Procedure, *Belgian Official Journal*, 24 December 2004, entry into force on 3 January 2005.

[199] Jan Kerkhofs and Philippe Van Linthout, *Cybercrime*, Brussels, Politeia, 2013, p. 184.

1) the indications and concrete facts specific to the case, which justify the measure under Article 90ter;
2) the reasons why the measure is necessary to reveal the truth;
3) the person, the (tele-)communications method or the place that is the subject of the monitoring measure;
4) the period during which the monitoring measure can be carried out, which should not be longer than one month counting from the decision by which the measure is ordered;
5) the name and the capacity of the judicial police officer designated for the implementation of the measure.

As said earlier, third parties do not have access to the judicial file (III.B.10.a.).

#### *c) Access of the defense to non-official reports*

According to Article 90*septies* §§6-8, the investigating judge or the court may allow the defendant, the accused, the civil party or their counsel upon request access to the whole or parts of the recordings deposited at the Registry (section III.B.3.a.aa.(1)).

#### *d) Right to request additional investigation methods*

As said above (section III.B.6.b.), on the basis of Article 61*quinquies* §1 CCP, the suspect and the civil party have the right to request the investigating judge to carry out additional investigation methods, such as the appointment of an expert or performance of a second test.[200]

According to Article 61*quinquies* §2 CCP, the suspect and the civil party shall submit their petition for an additional investigation method in writing to the Registry of the Court of First Instance. The petition should be substantiated and give a detailed description of the requested investigation method.

According to Article 61*quinquies* §3 CCP, the judge may reject the request if he considers the measures to be unnecessary in order to reveal the truth or if, at that moment, he considers the measures prejudicial to the investigation. According to Article 61*quinquies* §4 CCP, rejection by the investigating judge is subject to appeal before the Indictment Chamber (see section I.A.4.b.), in which case the investigating judge shall hear the Prosecutor General, the suspect, and his or her attorney (Article 61*quater* §5 CCP).

---

[200] Cf. Philip Traest, "Judicial control on the gathering and reliability of technical evidence in a continental criminal justice system", conference paper for the 16th International Conference of the International Society for the Reform of Criminal Law, 2002, p. 10, available at http://www.isrcl.org/Papers/Traest.pdf

Even though there is no explicit legal basis, the trial judge can also order the appointment of an expert or a second test at his own request or at the request of the parties. This power is included in the judge's general task of the finding of truth.[201]

### *e) Non-disclosure of technical means*

In a reply of 9 June 2011 to a parliamentary question (see section III.C.2.b.), the Minister of Justice explained that the use of "stealth" technology is allowed under Article 88*bis* CCP (tracing of traffic data, and localization of electronic communications). However, at the same time, the Minister of Justice recalled that the traditional prohibition of disclosure of the technical means used for special investigation methods, such as observation (Article 47*sexies* CCP; Article 47*octies* CCP), also holds for Article 88*bis* CCP, even though this measure concerns other investigation methods "in the area of the interception of telecommunications."[202] Hence, it could be asked to what extent the same rationale holds for the powers of looking-in operations (Articles 46*quinquies* and 89*ter* CCP) and the monitoring measure (Article 90*ter* CCP).

### *f) Exclusion of unreliable evidence*

Regarding the probity of intercepted data, the second Antigoon criterion is relevant, according to which illegally obtained evidence has to be excluded if the illegality has compromised the reliability of the evidence.

As noted above, both the Courts in Chambers, the Indictment Chamber, and the trial judge determine the grounds for finding a nullity on the basis of the so-called Antigoon criteria (see sections III.B.10.b. and IV.2.). If the Courts in Chambers finds no illegality and the parties do not appeal against this decision before the Court of Indictment, then they can raise this point again before the trial judge. If the parties appeal against this decision before the Indictment Chamber, then they cannot raise this point again before the trial judge, except if the alleged nullity concerns the weighing of evidence, which is an exclusive task of the trial judge (Article 235*bis* §5 CCP).

---

[201] Raf Verstraeten and Frank Verbruggen, *Straf- en strafprocesrecht voor bachelors* (Criminal law and criminal procedural law for bachelors), Antwerp-Apeldoorn, Maklu, 2007, p. 322.

[202] Belgian Chamber of Representatives, *Schriftelijke vragen en antwoorden* (written question and answers), 2010-2011, no. 53-032, p. 36, available at http://www.dekamer.be/QRVA/pdf/53/53K0032.pdf; see also Jan Kerkhofs and Philippe Van Linthout, *Cybercrime*, Brussels, Politeia, 2013, p. 258.

# V. Exchange of Intercepted Electronic Communication Data between Foreign Countries

## A. Legal Basis for Mutual Legal Assistance

### 1. International conventions

Belgium has ratified the following international conventions on mutual assistance applicable to the interception of electronic communications:

#### *a) UN conventions*

*United Nations Convention against Transnational Organized Crime of 15 November 2000*:[203] signature on 12 December 2000, ratification on 11 August 2004.[204] According to Article 38 §1 of the Convention (on entry into force), "[t]his Convention shall enter into force on the ninetieth day after the date of deposit of the fortieth instrument of ratification, acceptance, approval or accession." Hence, the Convention entered into force in Belgium on 9 November 2001.

Belgium made no declarations, reservations, or notifications specifically regarding the interception of electronic communications.[205]

#### *b) Council of Europe conventions*

*European Convention on Mutual Assistance in Criminal Matters of 20 April 1959* (CETS No. 030):[206] signature on 20 April 1959, ratification on 13 August 1975.[207] Article 27 §3 of the Convention provides: "As regards any signatory ratifying subsequently the Convention shall come into force 90 days after the date of

---

[203] United Nations Convention against Transnational Organized Crime, General Assembly Resolution 55/25 of 15 November 2000, the conventions and the protocols thereto are available at http://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-e.pdf

[204] Act of 24 June 2004 regarding the approval of the Convention against Transnational Organized Crime and its protocols, *Belgian Official Journal*, 13 October 2004, entry into force on 23 October 2004.

[205] The declarations and notifications by Belgium at the time of depositing (11 August 2004) the instrument of ratification of the United Nations Convention against Transnational Organized Crime are available here https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XVIII-12&chapter=18&lang=en#EndDec

[206] European Convention on Mutual Assistance in Criminal Matters, Strasbourg, 20 April 1959, available at http://conventions.coe.int/treaty/en/Treaties/Html/030.htm

[207] Act of 19 July 1975 regarding approval of the European Convention on Mutual Assistance in Criminal Matters of 20 April 1959, *Belgian Official Journal*, 23 October 1975, entry into force on 11 November 1975.

the deposit of its instrument of ratification." Hence, the Convention entered into force in Belgium on 11 November 1975.

Of note are the following reservations made by Belgium, at the time of depositing the instrument of ratification with the Secretary General of the Council of Europe, which cover the period since the entry into force of the Convention on 11 November 1975:

Concerning Article 2 of the Convention (on the refusal of assistance, under chapter I on general provisions):[208]

> The Government of the Kingdom of Belgium reserves the right not to comply with a request for assistance
>
> a. if there are good grounds for believing that it concerns an inquiry instituted with a view to prosecuting, punishing or otherwise interfering with an accused person because of his political convictions or religion, his nationality, his race or the population group to which he belongs;
> b. is so far as it concerns a prosecution or proceedings incompatible with the principle non bis in idem;
> c. in so far as it concerns an inquiry into acts for which the accused person is being prosecuted in Belgium.

Concerning Article 22 of the Convention (single article under chapter VII on the exchange of information from judicial records):

> The Government of the Kingdom of Belgium will not notify the subsequent measures referred to in Article 22 except in so far as the organisation of its judicial records allows of so doing.

Concerning Article 26 of the Convention (relation of the Convention to other legal instruments, under chapter VIII on final provisions):

> By reason of the special arrangements between the Benelux countries, the Government of the Kingdom of Belgium does not accept Article 26, paragraphs 1 and 3 in respect of its relations with the Netherlands and Luxembourg.
>
> The Government of the Kingdom of Belgium reserves the right to derogate from these provisions in respect of its relations with other member States of the European Economic Community.

Belgium also signed the two additional protocols to the *European Convention on Mutual Assistance in Criminal Matters:*

The *Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters*, 17 March 1978:[209] signature on 11 July 1978, ratification on

---

[208] The reservations and declarations made by Belgium at the time of depositing (13 August 1975) the instrument of ratification of the Convention on Mutual Assistance in Criminal Matters of 20 April 1959 are available here: http://conventions. coe.int/Treaty/Commun/ListeDeclarations.asp?CL=ENG&NT=030&VL=1

[209] Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters, Strasbourg, 17 March 1978, available at http://conventions.coe.int/treaty/en/Treaties/Html/099.htm

28 February 2002.[210] The additional protocol entered into force in Belgium on 29 May 2002.

*The Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters*, 8 November 2001:[211] signature on 8 November 2011, ratification on 9 March 2009.[212] The additional protocol entered into force in Belgium on 1 July 2009.

*Convention on Cybercrime* (CETS No. 185):[213] signature on 23 November 2001, ratification on 20 August 2012.[214] According to Article 36 §4 of the Convention:

> the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of the expression of its consent to be bound by the Convention.

Hence, the Convention entered into force in Belgium on 1 December 2012.

Belgium made no reservations or declarations specifically regarding the interception of electronic communications.[215]

### *c) EU conventions*

*Treaty between the Kingdom of Belgium, the Grand Duchy of Luxembourg and the Kingdom of the Netherlands concerning extradition and mutual assistance in criminal matters (Benelux Treaty)*, 27 June 1962:[216] signature on 27 June 1962, ratification on 30 July 1964.[217] Article 49 §2 of the Convention provides that "[t]he

---

[210] Act of 29 January 2002 regarding approval of the Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters, *Belgian Official Journal*, 1 June 2002, entry into force on 11 June 2002.

[211] Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters, Strasbourg, 8 November 2001, available at http://conventions.coe.int/treaty/en/Treaties/Html/182.htm

[212] Act of 8 November 2001 regarding approval of the Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters, *Belgian Official Journal*, 19 June 2009, entry into force on 1 July 2009.

[213] Cybercrime Convention, Budapest, 23 November 2001, available at http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm

[214] Act of 3 August 2012 regarding approval of the Cybercrime Convention, *Belgian Official Journal*, 21 November 2012, entry into force on 1 December 2012.

[215] The declaration of Belgium at the time of depositing (20 August 2012) the instrument of ratification of the Cybercrime Convention is available at http://conventions.coe.int/Treaty/Commun/ListeDeclarations.asp?NT=185&CM=&DF=&CL=ENG&VL=1

[216] Treaty between the Kingdom of Belgium, the Grand Duchy of Luxembourg and the Kingdom of the Netherlands concerning extradition and mutual assistance in criminal matters, Brussels, 27 June 1962, available at https://www.consilium.europa.eu/ueDocs/cms_Data/docs/polju/en/EJN220.pdf

[217] Act of 27 June 1962 regarding the approval of the Treaty between the Kingdom of Belgium, the Grand Duchy of Luxembourg and the Kingdom of the Netherlands concern-

Treaty shall enter into force two months after the deposit of the last instrument of ratification." Hence, the treaty entered into force on the same date for Belgium, Luxembourg, and the Netherlands. The Netherlands deposited the last instrument of ratification on 11 October 1967. Hence, the treaty entered into force two months later, on 11 December 1967.

Belgium made no declarations specifically regarding the interception of electronic communications.[218]

*Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union*, 29 May 2000:[219] signature on 29 May 2000, ratification on 25 May 2005.[220] Article 27 §§2–3 of the Convention read as follows:

> 2. Member States shall notify the Secretary-General of the Council of the European Union of the completion of the constitutional procedures for the adoption of this Convention. 3. This Convention shall, 90 days after the notification referred to in paragraph 2 by the State, member of the European Union at the time of adoption by the Council of the Act establishing this Convention, which is the eighth to complete this formality, enter into force for the eight Member States concerned.

Hence, the Convention entered into force in Belgium on 23 August 2005.

Belgium made no declarations specifically regarding the interception of electronic communications.[221]

Belgium also signed the additional protocol to the European Convention on Mutual Assistance in Criminal Matters:

*Protocol to the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union*, 16 October 2001:[222] signature on

---

ing extradition and mutual assistance in criminal matters, *Belgian Official Journal*, 24 October 1967, entry into force on 11 December 1967.

[218] The declarations of Belgium under the Benelux Treaty are available at the end of the Treaty: https://www.consilium.europa.eu/ueDocs/cms_Data/docs/polju/en/EJN220.pdf

[219] Council Act of 29 May 2000 establishing, in accordance with Article 34 of the Treaty on European Union, the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, OJ C 197, 12.7.2000, pp. 1-23.

[220] Act of 11 May 2005 regarding approval of the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, *Belgian Official Journal*, 22 June 2006, entry into force on 2 July 2005.

[221] The declaration of Belgium of 23 March 2011 under the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union is available at https://www.ejn-crimjust.europa.eu/ejn/libdocumentproperties.aspx?Id=18

[222] Protocol established by the Council in accordance with Article 34 of the Treaty on European Union to the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, OJ C 326, 21.11.2001, pp. 2–8.

16 October 2001, ratification on 25 May 2005.[223] The additional protocol entered into force in Belgium on 5 October 2005.

### 2. Bilateral Treaties

Article 25 §2 of the European Convention on Mutual Assistance in Criminal Matters of 20 April 1959 provides that "[t]he Contracting Parties may conclude between themselves bilateral or multilateral agreements on mutual assistance in criminal matters only in order to supplement the provisions of this Convention or to facilitate the application of the principles contained therein."

Accordingly, via letters signed on 6 March and 18 July 1975, Belgium and Germany concluded an additional bilateral agreement for cases in which the request for assistance concerns the following:

1) a civilly liable person who is involved in a criminal case, or
2) criminal investigations in fiscal matters (customs and excise, direct or indirect taxation, and exchange control).[224]

These cases were already provided in the provisions 2a-b of the additional protocol to the extradition and mutual legal assistance treaty between Belgium and Germany of 17 January 1958.[225]

### 3. National Regulation

Beyond the ratified treaties, Article 6 of the Act of 9 December 2004 concerning international mutual legal assistance in criminal matters lays down the general rules on international legal assistance in criminal matters (see above, section IV.3.c.):[226]

> §1. Requests for mutual legal assistance in criminal matters from the competent foreign authorities are implemented in accordance with Belgian law and, where appropriate, in

---

[223] Act of 11 May 2005 regarding approval of the Protocol to the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, *Belgian Official Journal*, 22.6.2005, entry into force on 2 July 2005.

[224] See Point 1.A of the agreement. An extract of the agreement is available on the website of the online legal database Vlex: http://vlex.be/vid/wisseling-brieven-belgi-bonds republiek-strafbare-30519154

[225] See the doctoral thesis of Professor Gert Vermeulen, *Wederzijdse rechtshulp in strafzaken in de Europese Unie* (mutual legal assistance in criminal matters in the European Union), Antwerp-Apeldoorn, Maklu, 1999, pp. 70–71, footnote 266; see also Gert Vermeulen, Tom Vander Beken, Els De Busser, Chris Van den Wyngaert, Guy Stessens, Adrien Masset, and Christophe Meunier, *Een nieuwe Belgisch wetgeving inzake internationale rechtshulp in strafzaken* (New Belgian legislation regarding international legal assistance in criminal matters), Antwerp-Apeldoorn, Maklu, 2002, p. 122, footnote 87.

[226] Act of 9 December 2004 regarding mutual assistance in criminal matters and modifying Article 90ter of the Code of Criminal Procedure, *Belgian Official Journal*, 24 December 2004, entry into force on 3 January 2005.

accordance with applicable international legal instruments that bind the requesting State and Belgium.

§2. However, if provided in the request for mutual legal assistance and if an international instrument that binds Belgium and the requesting State provides for such an obligation, the request shall be implemented in accordance with the procedural rules of the foreign authorities, provided that those rules do not restrict fundamental rights and without prejudice to any other principle of Belgian law.

§3. In the absence of an international instrument, that binds Belgium and the requesting State, and that provide for such an obligation, a request for mutual legal assistance may also, within the limits specified in §2, be implemented according to the procedural rules explicitly set out by the foreign authorities.

§4. If a request for mutual legal assistance cannot be implemented for legal reasons, then the responsible Belgian authorities immediately notify the competent foreign authorities with a reasoned decision and mention, where appropriate, the conditions under which implementation could still occur.

If a request for mutual legal assistance cannot be implemented within the timelines set, then the responsible Belgian authorities immediately notify the competent foreign authority, with a clear description of the reasons for the delay and the time within which implementation can take place.

Hence, Article 6 §4 of the Act of 9 December 2004 concerning international mutual legal assistance in criminal matters enables non-treaty based assistance for the interception of electronic communications.

## B. Requirements and Procedure (Including the Handling of Privileged Information)

### 1. Incoming requests

*a) Designation of authorities on the basis of Belgian law: no consent needed from the Belgian Minister of Justice for requests from EU Member States*

Article 5 §1 of the Act of 9 December 2004 concerning international mutual legal assistance in criminal matters provides that the consent of the Minister of Justice is not required for the implementation in Belgium of requests for mutual assistance from EU Member States.

However, Article 5 §2 of the Act of 9 December 2004 provides that the consent of the Minister of Justice is required when the request can be refused on the basis of one of the three reasons provided in Article 4 §1 of the same Act:

1) to reduce the risk that the death penalty will be imposed;
2) in case the suspect requests refusal of the mutual legal assistance request;
3) in case the requesting state does not give sufficient guarantees that the death penalty will not be pronounced or executed.

In these cases, Article 5 §3 of the Act provides that the Belgian judicial authorities, or the Prosecutor General in case the public prosecutor and the investigating judge received the request, shall send the foreign request to the Minister of Justice.

An *a contrario* reading of Article 5 §1 of the Act of 9 December 2004 means that the consent of the Minister of Justice is required for the implementation in Belgium of requests for mutual assistance from non-EU Member States.

Article 7 §1, 2° of the Act prescribes that requests for mutual assistance from foreign authorities shall be addressed to the Belgian judicial authorities via diplomatic channels. Belgium shall send the records relating to the implementation of the measure to the requesting state in the same way.

*b) Designation of authorities on the basis of international instruments*

Article 7 §2 of the Act of 9 December 2004 provides that an international instrument may prescribe that mutual legal assistance takes place either between the foreign authority and the Belgian judicial authorities or between the Ministries of Justice of the requesting state and Belgium.

However, Article 7 §4 of the Act of 9 December 2004 provides that, in case the foreign request concerns a case that can seriously harm the public order or essential interests of Belgium, the federal prosecutor, or the Prosecutor General in case the public prosecutor and the investigating judge received the request, shall immediately send an information report to the Minister of Justice.

Below, we apply this rule to the conventions on mutual legal assistance, mentioned earlier (section V.A.1.).

Two of the conventions regarding mutual legal assistance determine the competent authorities for implementing mutual legal assistance requests:

Article 15 of the *European Convention on Mutual Assistance in Criminal Matters of 20 April 1959* and Article 30 of the *Treaty between the Kingdom of Belgium, the Grand Duchy of Luxembourg and the Kingdom of the Netherlands concerning extradition and mutual assistance in criminal matters (Benelux Treaty) of 27 June 1962* determine the competent authorities for implementing mutual assistance requests.

The other two conventions allow the parties to designate the relevant authorities.

Belgium designated the Directorate-General legislation, fundamental rights and freedoms[227] of the Federal Public Service Justice as the competent authority under Article 18(13) of the United Nations Convention against Transnational Organized

---

[227] Directoraat-generaal Wetgeving en Fundamentele Rechten en Vrijheden (DG WL, in Dutch), Direction générale de la Législation et des Libertés et Droits fondamentaux (DG WL, in French).

Crime of 15 November 2000 and under Article 24 of the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union.[228]

Belgium designated the International Criminal Cooperation Department[229] of the Federal Public Service Justice as the competent authority under Article 24.7.a (making or receiving requests for extradition or provisional arrest) and Article 27.2 (sending and answering requests for mutual assistance) of the Cybercrime Convention:[230]

Belgium designated the Federal Computer Crime Unit (FCCU) of the Federal Judicial Police (Directorate for Combating Economic and Financial Crime) as the competent authority under Article 35 (24/7 point of contact) of the Cybercrime Convention.

### *c) Reporting duties to the Ministry of Justice*

Article 7 §3 of the Act of 9 December 2004 provides that the Belgian judicial authorities shall send a copy of every received request for mutual assistance to the Federal Public Service Justice.[231]

### *d) No filtering duties*

Belgian law does not subject the Belgian authorities to a duty to filter out or delete privileged information before transmitting the results of an interception measure to a foreign country (see section B.3.A.). As said above under this section, in special cases, the Minister of Justice will decide whether or not to respond to a foreign mutual legal assistance request.

---

[228] See the declaration of Belgium of 23 March 2011 under the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, available at https://www.ejn-crimjust.europa.eu/ejn/libdocumentproperties.aspx?Id=18

[229] Dienst Internationale Samenwerking in Strafzaken (in Dutch), Service de la coopération internationale pénale (in French).

[230] See the declaration of Belgium at the time of depositing (20 August 2012) the instrument of ratification of the Cybercrime Convention, available at http://conventions.coe.int/Treaty/Commun/ListeDeclarations.asp?NT=185&CM=&DF=&CL=ENG&VL=1

[231] Federale Overheidsdienst Justitie (in Dutch), Service Public Fédéral Justice (in French); see the notification by Belgium at the time of depositing (11 August 2004) the instrument of ratification of the United Nations Convention against Transnational Organized Crime, available at https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XVIII-12&chapter=18&lang=en#EndDec

## 2. Outgoing requests

### *a) Designation of authorities on the basis of Belgian law: consent needed from the Belgian Minister of Justice for requests from Belgium*

The principle of no consent by the Minister of Justice for requests from EU Member States, set forth in Article 5 §1 of the Belgian Act of 9 December 2004 concerning international mutual legal assistance in criminal matters, does not apply to mutual assistance requests from Belgian to EU Member States. Article 7 §1, 1° of the Act provides that the Belgian judicial authorities shall use diplomatic channels, via the Minister of Justice, to send the mutual assistance request as well as the records relating to the implementation of the measure to the foreign state.

### *b) Designation of authorities on the basis of international instruments*

Article 7 §2 of the Act of 9 December 2004 concerning international mutual legal assistance in criminal matters (regarding the designation of authorities by international instruments), as well as the exceptions thereto provided in Article 7 §4 of the same Act, also apply to cases of foreign requests for mutual assistance to Belgium (see section V.B.1.b.).

### *c) Exclusion of foreign evidence*

As said above (section IV.3.c.), Article 13 of the Act of 9 December 2004 regarding mutual assistance in criminal matters lays down the rules on the admissibility of intercepted data obtained from foreign jurisdictions. The first ground for excluding foreign evidence under Article 13 is the infringement of procedural requirements prescribed under sanction of nullity according to the law of the state where the evidence was obtained. Hence, there is no duty for Belgian authorities to delete information from foreign countries, which could not be intercepted according to Belgian laws.

## 3. Real-time transfer of communication data

Article 14, 2° of the Act of 9 December 2004 concerning international mutual legal assistance in criminal matters inserts §§6–7 into Article 90*ter* CCP (monitoring measure) (see also above: III.B.9.b.):

> §6. A competent foreign authority may, within the framework of a criminal investigation, temporarily wiretap, take cognizance of, and record private telecommunications during transmission, if the person to whom this measure applies is located on the Belgian territory and if the following conditions are fulfilled:
>
> 1° this measure requires no technical intervention of a body which is established in Belgium;
>
> 2° the foreign government has notified the measure to a Belgian judicial authority;

3° this possibility is provided in an international legal instrument between Belgium and the requesting State;

4° the decision of the investigating judge referred to in §7 has not yet been communicated to the foreign government concerned.

The information gathered under this paragraph can only be used on condition that the competent Belgian authority has agreed to the measure.

§7. Once the public prosecutor receives the notice referred to in paragraph 6, first section, 2 ° he immediately brings the notice to the investigating judge.

The investigating judge to whom a notice referred to in §6, first section, 2 ° is brought approves the measure if it is permissible in accordance with this article.

He informs the foreign government on his decision within ninety-six hours from its receipt by the Belgian judicial authorities.

In the event that additional time is necessary, the investigating judge may postpone its decision and its notification to the competent foreign authorities with a maximum of eight days. He shall immediately notify the competent foreign authority of this delay, stating the reasons.

If the investigating judge does not allow the measure referred to in §6, it shall also notify the foreign government that the gathered data must be destroyed and cannot be used.

The parliamentary preparatory works clarify that this provision implements Article 20 of the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union (see above, section V.A.1.).[232] Article 20 of the Convention refers to the interception of telecommunications without the technical assistance of another Member State and addresses situations in which the suspect either is situated in border areas where the networks of Belgian and foreign operators intertwine or uses satellite communication. In these cases, the requesting state can wiretap the communications as long as the requested state has not given a negative answer.

In a circular of 28 December 2005, the Board of Prosecutors General referred to the impossibility of applying the scenarios described in Article 18 of the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, which deals with wiretapping and immediate or subsequent transmission of telecommunications to the requesting state, and in Article 19 of the same Convention, which concerns access by foreign authorities to telecommunications services operated via a gateway on national territory via the intermediary of a designated service provider.[233]

---

[232] Parliamentary preparatory works, Chamber of Representatives, regarding international mutual assistance in criminal matters, 2003–2003, no. 51 1278/001, pp. 21–22, available at http://www.dekamer.be/FLWB/pdf/51/1278/51K1278001.pdf

[233] Board of Prosecutors General, Circular of 28 December 2005 on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, COL 15/2005, pp. 15–17, available (in Dutch and French) at http://www.om-mp.be/extern/getfile.php?p_name=3505798.PDF&pid=4226362

## C. European Investigation Order

The European Investigation Order[234](EIO) will pose challenges regarding electronic communications interception measures.

First, the EIO order will increase cases in which foreign law applies to evidence gathering on Belgian territory. We recall that Article 6 §2 of the Belgian Act of 9 December 2004 concerning international mutual legal assistance in criminal matters allows the implementation of foreign mutual assistance requests in accordance with foreign procedural law:

> if provided in the request for mutual legal assistance and if an international instrument that binds Belgium and the requesting State provides for such an obligation […], provided that those rules do not restrict fundamental rights and without prejudice to any other principle of Belgian law.

Furthermore, we noted that the annual reports of the Minister of Justice in implementation of Article 90*decies* CCP call for a modernization of the laws regarding the monitoring measures prescribed in Article 90*ter* (see section III.B.).[235] This call may resonate well with the observation of the Board of Prosecutors General that it is currently impossible for Belgium to realize immediate or subsequent transmission of electronic communications to a requesting state and to allow the latter state to access electronic communications services operated via a gateway on Belgian territory via the intermediary of a designated service provider (see the previous section V.B.3.).[236]

## D. Statistics

We did not receive a reply from the Ministry of Justice to our request to gain access to statistics or information on the extent of mutual legal assistance requests for electronic communications interception.

---

[234] The European Parliament and the Council of the European Union, Directive 2014/41/EU of the European Parliament and of the Council of the European Union of 3 April 2014 regarding the European Investigation Order in criminal matters, OJ L 130, 1.5.2014, pp. 1–36.

[235] See I.B.2.a. above. See, for instance, the 2013 annual report of the Minister of Justice in implementation of Article 90*decies* CCP, pp. 18, 47–48.

[236] Board of Prosecutors General, Circular of 28 December 2005 on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, COL 15/2005, pp. 15–17, available (in Dutch and French) at http://www.om-mp.be/extern/getfile.php?p_name=3505798.PDF&pid=4226362

# Bibliography*


Arnou, Luc, "Afluisteren tijdens het gerechtelijk onderzoek" (Wiretapping during the investigation); in Commentaar Strafrecht en strafvordering (Commentary criminal law and criminal procedural law), Gent, Kluwer, 2008, vol. 59, 95 pp.

Belgian Chamber of Representatives, *Schriftelijke vragen en antwoorden* (written questions and answers), 2010-2011, no. 53-032, 79 pp., available at http://www.dekamer.be/QRVA/pdf/53/53K0032.pdf

Belgian Institute for Postal Services and Telecommunications, "Synthese van de raadpleging door de raad van het bipt op verzoek van de minister voor ondernemen en vereenvoudigen van 29/04/2010 betreffende de praktische uitvoering van richtlijn 2006/24/EG van 15 maart 2006 (richtlijn betreffende de bewaring van gegevens)" (Summary regarding the implementation of the data retention directive 2006/24/EG of 15 March 2006), 2010, p. 14, available at http://www.bipt.be/public/files/nl/1259/3344_nl_2010-10-01_bipt-verslag_consultatie_data_retention-publieke_versie_v2010 1001_nl.pdf

Belgian Standing Intelligence Agencies Review Committee (Standing Committee I), "Activity reports", available (in Dutch and French) at http://www.comiteri.be/index.php ?option=com_content&view=article&id=40&Itemid=74&lang=EN

Board of Prosecutors General, "Telecommunicatierichtlijn inzake het opsporings- en vervolgingsbeleid betreffende inbreuken op de medewerkingsverplichtingen vervat in de artikelen 46bis §2, 88bis §2 en 90quater §2 van het wetboek van strafvordering" (Telecommunications Circular regarding the investigation and prosecution of violations of the cooperation duties under *Articles 46bis §2, 88bis §2 and 90 quater §2 CCP),* COL 14/2009, 17 December 2009, 11 pp., available (in Dutch and French) at http://www.om-mp.be/omzendbrief/4420834/col_14-2009_dd__17_12_2009.html

Board of Prosecutors General, Circular of 28 December 2005 on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, COL 15/2005, 26 pp., available (in Dutch and French) at http://www.om-mp.be/extern/getfile.php?p_name=3505798.PDF&pid=4226362

Board of Prosecutors General, Circular of 15 June 2005 regarding the Autonomic Police Treatment and the simplified official records, COL 8, available (in Dutch and French) at http://www.om-mp.be/omzendbrief/4016820/omzendbrief_col_8_d_d__15_06_2005.html

Bockstaele, Marc and others (eds.), *De Zoeking onderzocht* (An analysis of the search), Antwerp-Apeldoorn, Maklu, 2009, 403 pp.


---

* All URLs were last accessed in 10/2016.

Boulet, Gertjan, "Regulating Surveillance: The Belgian case," Deliverable 2.3 (The Legal Perspective) for the EU-funded project Increasing Resilience in Surveillance Studies (IRISS), pp. 49–52, 31 January 2013, available at http://irissproject.eu/wp-content/uploads/2013/04/Legal-perspectives-of-surveillance-and-democracy-report-D2.3-IRISS.pdf

Bourlet, Christina, "La lutte contre la fraude de mass: développements récents" (The fight against mass fraud: recent developments); in Dominique Grisay (ed.), *De la lutte contre la fraude à l'argent du crime: État des lieux,* Brussels, Groupe De Boeck, 2013, pp. 83–98.

Criminal Policy Service of the Ministry of Justice, reports in implementation of article 90*decies* CCP, available at http://www.dsb-spc.be/web/index.php?option=com_content&task=view&lang=nl&id=55

Cybersquad, presentation on the functions of Cybersquad, September 2012, available at https://www.b-ccentre.be/wp-content/uploads/2012/04/Cybersqu@d-28maart2012-v005.pdf

De Hert, Paul and Boulet, Gertjan, "The cooperation between Internet service/access providers and law enforcement authorities," country report for the Cybercrime Research Centre at Nicolaus Copernicus University (Poland), February 2015, 29 pp., available at http://www.cybercrime.umk.pl/files/files/Report%20Belgium_De%20Hert%20Boulet.docx

De Hert, Paul and Gutwirth, Serge, *Anthologie privacy/Anthologie de la vie privée* (Anthology of privacy), Academic and Scientific Publishers, 2013, 64 pp., available at http://www.anthologieprivacy.be/sites/anthology/files/documents/anthologie-privacy-asp_0.pdf

De Hert, Paul and Boulet, Gertjan, "Cybercrime report for Belgium," *International Review of Penal Law (RIDP / IRPL)*, 2013, issue 84, no. 1–2, pp. 12–59, available at http://www.penal.org/IMG/pdf/RIDP_2013_1_2_CD_Annexe.pdf, and *Electronic Review of the International Association of Penal* Law, 2013, http://www.penal.org/sites/default/files/files/RV-2.pdf

De Hert, Paul and Vermeulen, Mathias, "Toegang tot sociale media en controle door politie. Een eerste juridische verkenning vanuit mensenrechtelijk perspectief" (Access to social media and control by the police: a first legal exploration from the human rights perspective), *Panopticon*, 2012, vol. 33(2), pp. 258–272.

De Hert, Paul, "C.A.O. no. 81 en advies no. 10/2000 over controle van Internet en e-mail" (Labour law: Soft law on e-mail and Internet practices), *Rechtskundig weekblad*, 2002-2003, vol. 66/33, 19 April 2003, pp. 1281–1294.

De Hert, Paul and Van Leeuw, Frédéric, "Cybercrime Legislation in Belgium," in Eric Dirix and Yves-Henri Leleu (eds.), *The Belgian reports at the Congress of Washington of the International Academy of Comparative Law*, Brussels, Bruylant, 2011, pp. 867–956, available at http://www.vub.ac.be/LSTS/pub/Dehert/389.pdf

Delbrouck, Luk, "De proactieve recherche: een nieuw middel in de strijd tegen de georganiseerde criminaliteit?" (The proactive investigation: a new method in the fight against organized crime), *Jura Falconis*, 1999-2000, no. 1, 37 pp., available at https://www.law.kuleuven.be/jura/art/36n1/delbrouck.htm#N_136_

De Smet, Bart, "Voeging van strafdossiers op verzoek van de verdediging" (Adding a file at the request of the defense), *Rechtskundig Weekblad*, 2002–2003, p. 1022, annotation under Court of Appeal of Antwerp, 13 March 2002.

De Valkeneer, Christian, *Manuel de l'enquête pénale* (Manual on criminal investigation), Brussels, Larcier, 2006, 498 pp.

De Wolf, Daniel, "Rapport Belge" (Belgian report on criminal procedure), *Electronic Review of the International Association of Penal Law*, 2014, 52 pp., available at http://www.penal.org/sites/default/files/files/RA%20-%203.pdf

Dewandeleer, Dirk, "De kennisname van e-mails 'tijdens de overbrenging ervan', een verduidelijking van het telecommunicatiegeheim" (Taking knowledge of e-mails during the transmission phase. A clarification of the secrecy of telecommunications), annotation to the judgment of the Correctional Court of Leuven, 4 December 2007, *Tijdschrift voor Strafrecht*, 2008, vol. 3, pp. 226–231.

Dupont, Lieven, *Beginselen van strafrecht Deel 1* (Principles of criminal law vol. 1), Leuven, Acco, 2004, 229 pp.

Eubelius: "Legal Embedment of the Antigoon case law", December 2013, available at http://www.eubelius.be/en/spotlight/legal-embedment-antigoon-case-law

European Telecommunications Standards Institute, "TS 101-331 Lawful Interception (LI); Requirements of Law Enforcement Agencies," V1.1.1 (2001-08), 4.7.g, available at http://www.etsi.org/deliver/etsi_TS/101300_101399/101331/01.01.01_60/ts_101331v010101p.pdf

Facebook, "Government requests reports," available via https://govtrequests.facebook.com/

Federal Prosecutor's Office, Annual Report of the Public Prosecutor's Office to the Board of Prosecutors General for the period of 1 January 2012 till 23 December 2012, 2012, p. 124, available (in Dutch) at http://www.om-mp.be/images/upload_dir/jaarverslag2012.pdf

Federal Science Policy Office (BELSPO), "Stated goals van autonome afhandeling door de politie (APA): zijn ze opportuun en worden ze bereikt?" (Stated goals of the Autonomic Police Treatment: are they opportune and have they been achieved?), dissemination activities of a government-funded research project on the opportunity of APT and evaluation of its effectiveness, from 1 December 2000 till 28 February 2003, SO/02/016, available via http://www.belspo.be/belspo/fedra/proj.asp?l=nl&COD=SO%2F02%2F016

Freyne, Thierry, "De bewaking van privécommunicatie en -telecommunicatie in strafonderzoeken: een stand van zaken" (The monitoring of private communications and telecommunications in criminal proceedings: a state of affairs), *Tijdschrift voor Strafrecht,* 2008, vol. 3, pp. 165–182.

Google, "Transparency Reports", available via http://www.google.com/transparencyreport/?hl=en_US

Goossens, Franky, *Politiebevoegdheden en mensenrechten in België. Rechtsvergelijkend en internationaal onderzoek* (Police powers and human rights in Belgium. Comparative and international research), doctoral thesis, Leuven, 2006, 778 pp., available at https://lirias.kuleuven.be/bitstream/1979/420/2/frankydoctoraat.pdf

Kennes, Laurent, *Manuel de la preuve en matière pénale* (Manual on evidence in criminal matters), Mechelen, Kluwer, 2009, 443 pp.

Kerkhofs, Jan and Van Linthout, Philippe, *Cybercrime*, Politeia, Brussels, 2013, 639 pp.

Konings, Charlotte and Oerlemans, Jaap-Jan, "Van een netwerkzoeking naar online doorzoeking: grenzeloos of grensverleggend" (From a network search to an online search: borderless or groundbreaking?), *Computerrecht*, 2013, vol. 5, pp. 23–32, available at https://www.b-ccentre.be/download/b-ccentre_legal/B-CCENTRE%20Van%20een%20netwerkzoeking%20naar%20online%20doorzoeking.pdf

Microsoft, "Law Enforcement Requests Reports", available at https://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency/

National Labour Council, "National collective agreement no. 81 of 26 April 2002 on the protection of the private lives of employees with respect to controls on electronic on-line communications data", 26 April 2002, available via www.cnt-nar.be

Parliamentary preparatory works, Chamber of Representatives, regarding international mutual assistance in criminal matters, 2003–2003, no. 51 1278/001, 53 pp., available at http://www.dekamer.be/FLWB/pdf/51/1278/51K1278001.pdf

Parliamentary preparatory works, Belgian Chamber of Representatives, regarding special investigation methods and any other methods of investigation, 2001–2002, no. 50 1688/001, 193 pp., available via http://www.senate.be/www/?MIval=dossier&LEG=2&NR=1260&LANG=nl

Parliamentary preparatory works, modifying the Act of 30 June 1994 protecting privacy against the interception of communication and telecommunication, Belgian Chamber of Parliaments, 1996-1997, 29 May 1998, no. 49K1075/017, p. 10, available at http://www.dekamer.be/FLWB/PDF/49/1075/49K1075017.pdf

Parliamentary preparatory works, regarding the legislative proposal protecting privacy against the interception of communication and telecommunication, Belgian Senate, 1993-1994, 18 May 1994, no. 843-2, 346 pp., available at http://www.senate.be/lexdocs/S0539/S05390364.pdf

Parliamentary preparatory works, regarding the legislative proposal protecting privacy against the interception of communication and telecommunication, Belgian Senate, 1992–1993, 1 September 1993, no. 843-1, 67 pp., available at http://www.senate.be/lexdocs/S0539/S05390297.pdf

Pesquié, Brigitte (revised by Yves Cartuyvels), "The Belgian system", in Mireille Delmas-Marty and J.R. Spencer, *European Criminal Procedures*, Cambridge Studies in International and Comparative Law, Cambridge University Press, 2002, pp. 81–141.

Silva, Karine and Roex, Ruben, "Zombie alert: Assessing legitimacy of P2P botnet mitigation techniques", 2014, conference paper, 25th European Regional Conference of the International Telecommunications Society (ITS), Brussels, Belgium, 22–25 June 2014, 13 pp., available at http://econstor.eu/bitstream/10419/101402/1/795035411.pdf

Traest, Philip, "Judicial control on the gathering and reliability of technical evidence in a continental criminal justice system", conference paper for the 16th International Conference of the International Society for the Reform of Criminal Law, 2002, 13 pp., available at http://www.isrcl.org/Papers/Traest.pdf

Traest, Philip, "Rechts(on)zekerheid in materieel en formeel strafrecht en strafrechtelijk legaliteitsbeginsel" (Legal (un)certainty in material and formal criminal law, and the principle of legality in criminal law), *Rechtskundig Weekblad*, 1993–1994, pp. 1190–1207.

Twitter, "Transparency reports", available via https://transparency.twitter.com/

Voet, Stefaan, "Belgium's new specialized judiciary," *Russian Law Journal*, 2014, vol. II, Issue 4, pp. 129–145, available at http://www.russianlawjournal.org/index.php/jour/article/view/14/10

Van den Wyngaert, Chris, *Strafrecht, Strafprocesrecht & Internationaal Strafrecht in hoofdlijnen* (An Outline of Criminal Law, Criminal Procedural Law & International Criminal Law), Antwerp-Apeldoorn, Maklu, 2006, 1314 pp.

Verizon, "Transparency Reports", available via http://transparency.verizon.com/

Vermeulen, Gert, *Wederzijdse rechtshulp in strafzaken in de Europese Unie* (Mutual legal assistance in criminal matters in the European Union), Antwerp-Apeldoorn, Maklu, 1999, 632 pp.

Vermeulen, Gert, Vander Beken, Tom, De Busser, Els, Van den Wyngaert, Chris, Stessens, Guy, Masset, Adrien, and Meunier, Christophe, *Een nieuwe Belgisch wetgeving inzake internationale rechtshulp in strafzaken* (New Belgian legislation regarding international legal assistance in criminal matters), Antwerp-Apeldoorn, Maklu, 2002, 421 pp.

Verstraeten, Raf, *Handboek strafvordering* (Manual on criminal procedure), Antwerp, Maklu, 2007, 1193 pp.

Verstraeten, Raf and Verbruggen, Frank, *Straf- en strafprocesrecht voor bachelors* (Criminal law and criminal procedural law for bachelors), Antwerp-Apeldoorn, Maklu, 2007.

Vodafone, "Law Enforcement Disclosure Report," 2014, available at http://www.vodafone.com/content/sustainabilityreport/2014/index/operating_responsibly/privacy_and_security/law_enforcement.html

The Washington Post, "Do France and Belgium have direct wiretap access to telecom switches?," 7 June 2014, available at http://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/06/07/do-france-and-belgium-have-direct-wiretap-access-to-telecom-switches/

## List of Abbreviations

| | |
|---|---|
| ADIV | Algemene Dienst Inlichtingen en Veiligheid (General Intelligence and Security Service of the Armed Forces) |
| APA | Autonome Politionele Afhandeling (Traitement Policier Autonome/Autonomic Police Treatment) |
| APO | Ambtshalve Politioneel Onderzoek (Enquête Policière d'Office/Autonomic Police Treatment) |
| APT | Autonomic Police Treatment |

| | |
|---|---|
| BBI | Bijzondere belastinginspectie (Special Tax Inspectorate) |
| BIPT | Belgian Institute for Postal Services and Telecommunications |
| BELSPO | Federal Science Policy Office |
| BISC | Belgian Internet Service Center |
| CC | Criminal Code |
| CCP | Code of Criminal Procedure |
| CETS | Convention on Cybercrime |
| CFI | Cel voor Financiële Informatieverwerking (Belgian Financial Intelligence Processing Unit) |
| Comité P | Vast Comité van toezicht op de politiediensten (Comité permanent de contrôle des services de police/ Standing Police Monitoring Committee) |
| CTIF | Cellule de Traitement des Informations Financières (Financial Intelligence Processing Unit) |
| DNS | Domain Name Service |
| EC | European Commission |
| ECHR | European Convention on Human Rights |
| ECtHR | European Court of Human Rights |
| FOD | Federale Overheidsdienst (Federal Public Service) |
| ISI | Inspection spéciale des impôts (Special Tax Inspectorate |
| ISP | Internet Service Provider |
| GISS | General Intelligence and Security Service of the Armed Forces |
| IMEI | International Mobile Station Equipment Identity |
| IMSI | International Mobile Subscriber Identity |
| LEMF | Law Enforcement Monitoring Facility |
| NTSU-CTIF | National Technical & Tactical Support Unit – Central Technical Interception Facility |
| SIM-commission | Administrative Commission responsible for monitoring the specific and exceptional intelligence collection methods used by the intelligence and security services |
| SGRS | Service général du Renseignement et de la Sécurité (General Intelligence and Security Service of the Armed Forces) |
| SPF | Service Public Fédéral (Federal Public Service) |
| Standing Committee I | Belgian Standing Intelligence Agencies Review Committee |
| VSSE | Veiligheid van de Staat / La Sûreté de l'Etat |